SOPHOS

Security made simple.

Sophos Reporting Interface
Guide d'utilisation

Version du produit : 5.2

Date du document : janvier 2013

Table des matières

1 À propos de ce guide

Ce guide vous explique comment Sophos Reporting Interface vous permet d'utiliser le logiciel tiers d'édition de rapports pour créér des rapports à partir des données de menaces et d'événements dans Sophos Enterprise Console. Il s'adresse aux administrateurs système et aux administrateurs de base de données.

Ce guide suppose que vous connaissez et utilisez déjà la version 5.2 de Sophos Enterprise Console (SEC).

Remarque : si vous voulez exporter des données dans des applications tierces de surveillance de journaux, comme Splunk, vous pouvez le faire à l'aide de Sophos Reporting Log Writer. Retrouvez plus de renseignements dans le *Guide d'utilisation de Sophos Reporting Log Writer*.

Retrouvez la documentation Sophos sur http://www.sophos.com/fr-fr/support/documentation.aspx.

2 Qu'est-ce que Sophos Reporting Interface ?

Sophos Reporting Interface sert à générer des rapports détaillés et personnalisés sur les ordinateurs d'extrémité administrés par la Sophos Enterprise Console.

Sophos Reporting Interface permet aux applications tierces comme Crystal Reports et SQL Reporting Services d'accéder aux données présentes sur le serveur SQL stockées par l'Enterprise Console. Les objets de base de données requis sont installés dans le cadre de l'installation de la base de données Enterprise Console.

3 À propos de l'utilisation de Sophos Reporting Interface

Important : Sophos Reporting Interface met les données de l'Enterprise Console à disposition des applications tierces. Ces données peuvent contenir des informations confidentielles sur vos utilisateurs et vos ordinateurs. En utilisant Sophos Reporting Interface, vous assumez la responsabilité de la sécurité des données mises à disposition et garantissez également que seuls les utilisateurs autorisés ont accès à ces données.

Par ailleurs, en plus de limiter l'accès aux données récupérées par Sophos Reporting Interface, nous vous conseillons vivement de chiffrer les connexions entre les clients et la base de données de l'Enterprise Console. Retrouvez plus de renseignements dans la documentation de SQL Server :

- Activer les connexions chiffrées dans le moteur de base de données (Gestionnaire de configuration SQL Server), SQL Server 2012
- Chiffrement des connexions à SQL Server 2008 R2
- Comment faire pour activer le chiffrement SSL pour une instance de SQL Server à l'aide de la console MMC, SQL Server 2005

Remarque :

- Dans certains environnements système, les requêtes supplémentaires faites à la base de données de l'Enterprise Console pendant l'accès au Reporting Interface pourraient avoir un impact sur les performances d'autres opérations de base de données. Les performances de l'Enterprise Console peuvent diminuer sensiblement lors d'importants transferts de données depuis Reporting Interface.
- Nous vous conseillons d'utiliser les ID numériques plutôt que des valeurs de chaînes si vous voulez relier toute logique externe aux données récupérées par Reporting Interface. Ceci permettra d'éviter tout problème potentiel de compatibilité en cas de modification des valeurs de chaînes dans une future édition de l'Enterprise Console.

Vous pouvez utiliser Reporting Interface avec des applications tierces telles que Microsoft Excel, Microsoft Access, Microsoft SQL Server Reporting Services ou Crystal Reports.

Retrouvez un exemple d'utilisation de Crystal Reports pour accéder à Reporting Interface à l'Annexe : à la page 14. configuration de Crystal Reports avec Reporting Interface à la page 14.

Retrouvez plus de renseignements sur l'utilisation de vos propres outils de rapports sur le fil de discussion de Sophos Reporting Interface du forum de la communauté SophosTalk.

4 Quelles informations sont accessibles ?

Sophos Enterprise Console enregistre les informations sur les :

- Ordinateurs
- Packages
- Groupes
- Événements
- Menaces

4.1 Ordinateurs

Les ordinateurs sont les ordinateurs d'extrémité individuels surveillés par l'Enterprise Console et uniquement identifiés par leur identifiant *ComputerID*. Vous pouvez accéder aux informations sur les ordinateurs à l'aide des vues de base de données suivantes :

- **vComputerHostData** fournit des informations sur chaque ordinateur surveillé par l'Enterprise Console.
- **vPolicyComplianceData** dresse une liste des stratégies appliquées à chaque ordinateur ainsi que l'état de conformité à ces stratégies.

4.2 Groupes

Les groupes sont un regroupement logique d'ordinateurs effectué depuis l'Enterprise Console qui sont uniquement identifiés par *GroupID*. Vous pouvez accéder aux informations sur les groupes à l'aide des vues de base de données suivantes :

- **vGroupPathAndNameData** fournit une liste de chemins de groupes.
- **vComputerGroupMapping** dresse la liste des ordinateurs et les groupes auxquels ils appartiennent.

4.3 Packages

Les packages sont des versions particulières de Sophos Anti-Virus qui peuvent être présentes sur le réseau et qui sont uniquement identifiées par *PackageID*. Vous pouvez accéder aux informations sur les packages à l'aide des vues de base de données suivantes :

- **vPackageData** dresse une liste des versions de Sophos Anti-Virus actuellement disponibles ou qui étaient disponibles.
- **vComputerPackageMapping** indique quel package est installé sur chaque ordinateur.

4.4 Événements

Les événements sont des notifications d'événements qui se sont produits sur les ordinateurs d'extrémité et qui sont uniquement identifiés à la fois par leurs identifiants *EventID* et *EventTypeID*.

Les événements sont classés par type dans différentes catégories. **vEventsCommonData** fournit des informations de base sur tous les événements qui se sont produits et inclut un **EventTypeName** pour indiquer laquelle des vues suivantes contiendra des informations spécifiques aux catégories sur l'événement :

- Contrôle des applications avec **vEventsApplicationControlData**
- Contrôle des données avec **vEventsDataControlData**
- Contrôle des périphériques avec **vEventsDeviceControlData**
- Pare-feu avec **vEventsFirewallData**
- Protection antialtération avec **vEventsTamperProtectionData**
- Contrôle du Web avec **vEventsWebData**
- Actions contre les menaces avec **vThreatEventData**

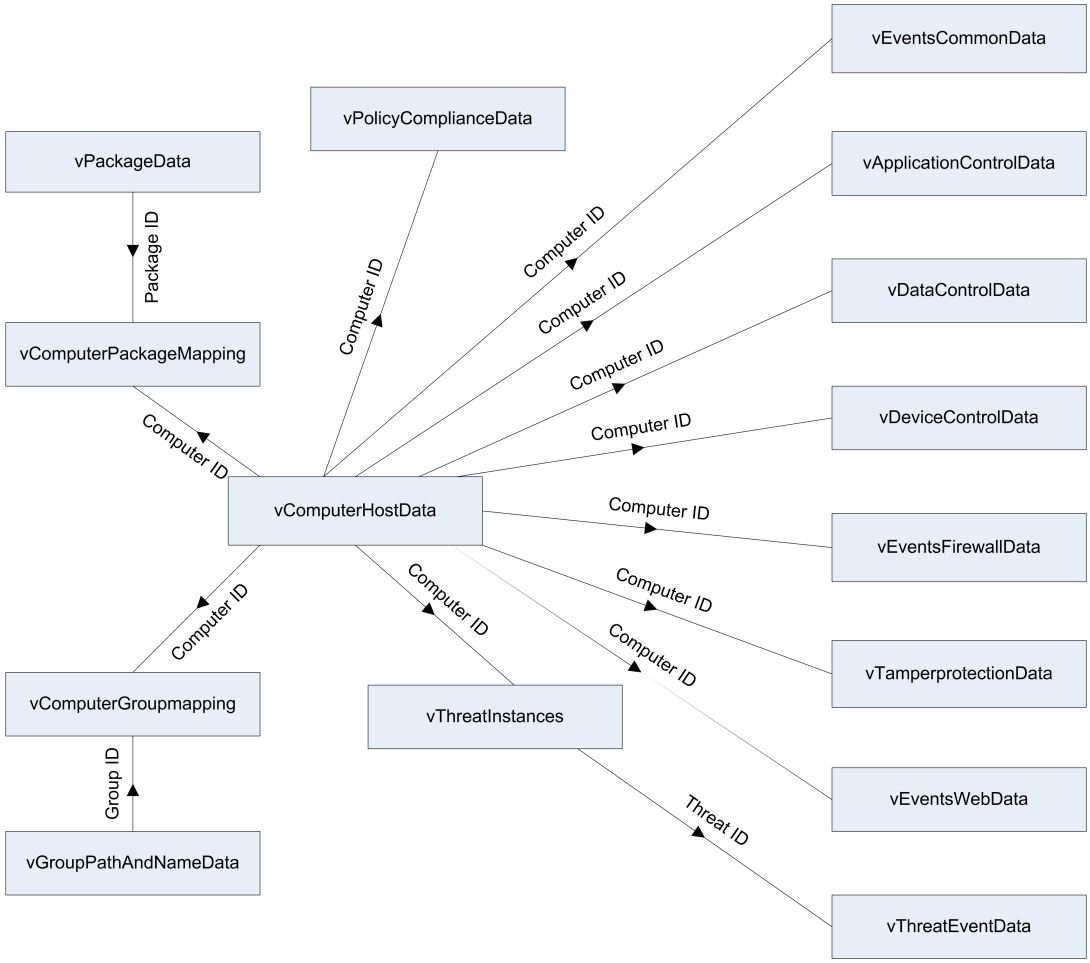
4.5 Menaces

Les menaces sont des fichiers ou des applications identifiés comme appartenant à une des catégories d'éléments à risque (virus/spywares, fichiers/comportements suspects, adwares et PUA). Ils sont identifiés exclusivement par *ThreatID*. Vous pouvez accéder aux informations sur les menaces à l'aide des vues de base de données suivantes :

- **vThreatInstances** dresse la liste des menaces qui ont été détectées sur chaque ordinateur.
- **vThreatEventData** fournit une liste des actions effectuées pour répondre aux menaces détectées sur le réseau.

4.6 Quelles sources de données sont liées ?

Lors de la fusion de données à partir de plusieurs vues, les lignes de chaque vue faisant référence à la même entité doivent être jointes. Cette opération s'effectue en joignant les lignes qui font référence aux numéros d'identification de la même entité. Le schéma suivant montre les champs à utiliser pour joindre chacune des vues disponibles.


vEventsCommonData
vPolicyComplianceData
vPackageData
vApplicationControlData
Package ID
Computer ID
Computer ID
vDataControlData
vComputerPackageMapping
Computer ID
Computer ID
vDeviceControlData
Computer ID
vComputerHostData
Computer ID
vEventsFirewallData
Computer ID
Computer ID
Computer ID
vTamperprotectionData
vComputerGroupmapping
Computer ID
vThreatInstances
Group ID
vEventsWebData
Threat ID
vGroupPathAndNameData
vThreatEventData

5 Sources de données Reporting Interface

Les sources de données suivantes sont disponibles pour Reporting Interface.

Remarque : une lettre de l'alphabet figurant à côté d'une source de données est utilisée pour représenter la source de données dans le tableau ci-dessous.

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

Le tableau suivant vous indique quels champs de données sont disponibles pour chaque source de données. Toutes les colonnes date-heure sont rapportées en Temps Universel Coordonné (UTC, Universal Coordinated Time) au format « aaaa-mm-jj hh:mi:ss »" (24 heures).

Champ de données	Type de données	Source de données														
		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			•	•	•	•	•	•	•						

Champ de données	Type de données	Source de données														
		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		•	•	•	•	•	•	•	•	•					
Domain	nvarchar	•														
IPAddress	nvarchar	•														
Description	nvarchar	•														
LastMessageReceived Time	nvarchar	•														
DNSName	nvarchar	•														
OperatingSystemID	integer	•														
OperatingSystem Name	nvarchar	•														
ServicePack	nvarchar	•														
ThreatTypeID	integer		•													
ThreatTypeName	nvarchar		•													
ThreatSubTypeID	integer		•													
ThreatSubTypeName	nvarchar		•													

Champ de données	Type de données	Source de données														
		A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
Priority	integer		•													
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						•									
Model	nvarchar						•									
DeviceID	integer						•									
Role	nvarchar							•								
FileName	nvarchar							•								
FilePath	nvarchar							•								
FileVersion	nvarchar							•								

Champ de données	Type de données	Source de données													
		A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
FileChecksum	nvarchar							•								
CommandLine	nvarchar							•								
Session	nvarchar							•								
Desktop	nvarchar							•								
Emplacement	nvarchar							•								
ProtocolID	integer							•								
ProtocolText	nvarchar							•								
DirectionID	integer							•								
DirectionText	nvarchar							•								
LocalAddress	nvarchar							•								
RemoteAddress	nvarchar							•								
LocalPort	integer							•								
RemotePort	integer							•								
TargetTypeID	integer								•							
TargetTypeText	nvarchar								•							
Cible	nvarchar								•							
RuleID	integer									•						
BlockedSite	nvarchar									•						
ReferringURL	nvarchar									•						
ReasonID	integer									•						
ReasonName	nvarchar									•						
CategoryID	integer									•						
CategoryName	nvarchar									•						

Champ de données	Type de données	Source de données														
		A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
ActionTakenID	integer										•					
ActionTakenName	nvarchar										•					
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 Annexe : configuration de Crystal Reports avec Reporting Interface

Cet exemple illustre l'utilisation de la version 2008 ou supérieure de Crystal Reports pour accéder à Reporting Interface.

L'assistant Crystal Reports reliera automatiquement les colonnes à des noms identiques entre les vues qui ont été incluses dans un rapport. Par contre, certaines des connexions doivent être supprimées car les colonnes nommées de manière similaire n'ont pas nécessairement des valeurs identiques pour un seul événement de journal.

Par exemple, la colonne **InsertedAt** est présente dans chaque vue qui indique quand chaque entrée a été ajoutée dans la base de données. Par contre, un seul événement peut avoir différentes heures **InsertedAt** pour ses entrées correspondantes dans chaque vue. Si l'assistant Crystal Reports relie automatiquement ces colonnes, les liens doivent être supprimés pour empêcher les données manquantes. Retrouvez plus de renseignements sur les sources de données liées à la section Quelles sources de données sont liées ? à la page 7.

Pour créer une connexion Reporting Interface avec Crystal Reports :

1. Ouvrez Crystal Reports et créez une nouvelle connexion à l'aide d'**OLE DB (ADO)** et choisissez **Microsoft OLE DB Provider for SQL Server**.
2. Saisissez les informations de connexion et suivez toutes les étapes de l'assistant.

   Sophos Reporting Interface apparaîtra désormais dans la liste des sources de données disponibles. Retrouvez plus de renseignements sur la création de rapports personnalisés dans la documentation Crystal Reports.

Retrouvez une liste des sources de données disponibles pour Reporting Interface à la section Sources de données Reporting Interface à la page 9.

Retrouvez plus de renseignements et d'exemples sur l'utilisation de Crystal Reports pour accéder aux données fournies par Sophos Reporting Interface dans l'article 112873 de la base de connaissances http://www.sophos.com/fr-fr/support/knowledgebase/112873.aspx.

7 Support technique

Vous bénéficiez du support technique des produits Sophos de l'une des manières suivantes :

- Rendez-vous sur le forum Sophos Community en anglais sur community.sophos.com/ et recherchez d'autres utilisateurs rencontrant le même problème que le vôtre.
- Rendez-vous sur la base de connaissances du support de Sophos sur www.sophos.com/fr-fr/support.aspx.
- Téléchargez la documentation des produits sur www.sophos.com/fr-fr/support/documentation.aspx.
- Ouvrez un incident support sur https://secure2.sophos.com/fr-fr/support/contact-support/support-query.aspx.

8 Mentions légales