SOPHOS

Cybersecurity made simple.

Sophos Enterprise Console

Guide d’utilisation de la fonction d’audit

Version du produit : 5.5

Table des matières

1 À propos de ce guide

Ce guide vous indique comment suivre tous les changements apportés à la configuration de Sophos Enterprise Console et toutes les actions effectuées par l'utilisateur ou par le système.

2 À propos de Sophos Auditing

Sophos Auditing vous permet de surveiller et suivre tous les changements apportés à la configuration de l'Enterprise Console et toutes les actions effectuées par l'utilisateur ou par le système. Vous pouvez utiliser ces informations afin de rester en conformité aux normes réglementaires et afin de résoudre les problèmes. Vous pouvez également vous en servir pour étayer une analyse juridique en cas d'activité malveillante.

Par défaut, l'audit est désactivé. Après avoir activé l'audit dans l'Enterprise Console, une entrée d'audit est écrite dans la base de données SQL Server nommée SophosSecurity à chaque fois que certains paramètres de configuration sont changés ou que certaines actions sont effectuées.

L'entrée d'audit inclut les informations suivantes :

- Action effectuée
- Utilisateur qui a effectué l'action
- Ordinateur de l'utilisateur
- Sous-parc de l'utilisateur
- Date et heure de l'action

Toutes les tentatives réussies ou ratées font l'objet d'un audit. Par conséquent, les entrées d'audit peuvent afficher les actions effectuées sur le système et l'identité de l'utilisateur qui a lancé les actions qui ont échoué.

Vous pouvez utiliser des programmes tiers tels que Microsoft Excel, Microsoft Access, Microsoft SQL Server Reporting Services ou Crystal Reports pour accéder et analyser les données stockées dans la base de données d'audit.

Important
Sophos Auditing met les données à disposition des applications tierces. En utilisant cette fonction, 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. Retrouvez plus de renseignements sur la sécurité à la section Protection de la base de données intégrée (page 4).

Retrouvez plus de renseignements sur les actions faisant l'objet d'un audit à la section Quelles actions sont soumises à l'audit ? (page 22).

3 Étapes essentielles à suivre lors de l’utilisation de Sophos Auditing

Les étapes essentielles à suivre lors de l’utilisation de Sophos Auditing sont :

- Sécurisation de la base de données
- Activation de la fonction d’audit
- Autorisation d’accès aux données d’audit
- Création d’un rapport d’audit

4 Sécurisation de la base de données

4.1 Protection de la base de données intégrée

L'Enterprise Console et la base de données SophosSecurity offre plusieurs types intégrés de protection pour les données d'audit :

- Contrôle d'accès
- Protection antialtération

Contrôle d'accès

Le contrôle d'accès est mis en place aux niveaux suivants :

- Niveau de l'interface utilisateur graphique (GUI)

  Seuls les utilisateurs disposant des droits d'**Audit** dans l'Enterprise Console et qui sont membres du groupe Sophos Console Administrators peuvent activer ou désactiver la fonction d'audit.

- Niveau de la base de données

  Par défaut, seuls les utilisateurs qui sont membres du groupe Sophos DB Admins peuvent accéder aux interfaces de la base de données. En outre, les procédures stockées à partir des interfaces de la base de données nécessitent la présentation d'un token de session utilisateur valide. Le token est généré par le système lorsqu'un utilisateur ouvre la GUI ou change le sous-parc.

Protection antialtération

La base de données est conçue pour empêcher toutes modifications des données d'événements d'audit. Hormis certains paramètres de configuration, il n'est pas nécessaire de mettre à jour les données de la base de données d'audit. Des déclencheurs sont présents pour annuler toutes tentatives de mise à jour ou de suppression des données dans les tableaux.

Les données peuvent uniquement être supprimées en procédant au nettoyage de la base de données. Les données de plus de deux ans sont automatiquement éliminées toutes les 24 heures dans le cadre de la tâche de nettoyage planifiée intégrée sur le serveur de l'Enterprise Console. Vous pouvez également utiliser l'outil PurgeDB pour nettoyer les données. Retrouvez plus de renseignements sur http://www.sophos.com/fr-fr/support/knowledgebase/109884.aspx.

4.2 Renforcement de la sécurité de la base de données

Audit de la base de données

En plus de la protection intégrée aux bases de données , nous vous conseillons de paramétrer la protection supplémentaire au niveau de l'instance SQL Server (s'il n'est pas déjà en place) pour auditer les activités de l'utilisateur et les modifications qu'il a effectué sur votre SQL Server.

Par exemple, si vous utilisez une édition Enterprise de SQL Server 2008, vous pouvez utiliser la fonction SQL Server Audit. Des versions précédentes de SQL Server prennent en charge l'audit de connexion, l'audit par déclencheur externe et l'audit des événements à l'aide d'un utilitaire de suivi intégré.

Retrouvez plus de renseignements sur les fonctions que vous pouvez utiliser pour procéder à l'audit des activités et des modifications sur votre système SQL Server dans la documentation correspondant à votre version de SQL Server. Par exemple :

- SQL Server Audit (moteur de base de données)
- Audit (moteur de base de données), SQL Server 2008 R2
- Audit dans SQL Server 2008
- Audit (moteur de base de données), SQL Server 2008

Chiffrement des connexions à la base de données

Nous vous conseillons fortement de chiffrer les connexions entre tous les clients et la base de données . 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)
- 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

Contrôle de l'accès aux copies de sauvegardes de la base de données

Assurez-vous qu'un contrôle d'accès correct et restrictif aux copies de sauvegarde de la base de données est mis en place. Ceci permet de garantir que les utilisateurs non autorisés n'auront pas accès aux fichiers, ne pourront pas les altérer ou les supprimer accidentellement.

Remarque
Les liens de cette section vous dirigent vers des informations mises à jour par des tiers et sont fournies pour vous aider. Même si nous vérifions régulièrement l'exactitude de ces liens, il se peut que ceux-ci soient modifiés sans que nous en ayons connaissance.

Vérification de la connexion à la base de données

Lors de l'exécution du programme d'installation de 5.5.1, les vérifications de la connexion à la base de données sont effectuées (avant l'installation ou la mise à niveau) afin de déterminer si une connexion peut être établie à la base de données à l'aide de TLS 1.2.

Pour vous assurer que TLS 1.2 est bien utilisé pour établir la connexion à la base de données, veuillez utiliser l'outil **CheckDBConnection.exe** afin de fournir la sortie sur les vérifications de la connexion et procéder à des modifications manuelles.

Retrouvez plus de renseignements dans l'article 127521 de la base de connaissances.

5 Activation de Sophos Auditing

Par défaut, l'audit est désactivé. Pour activer l'audit :

1. Dans l'Enterprise Console, dans le menu **Outils**, cliquez sur **Gérer l'audit**.
2. Dans la boîte de dialogue **Gestion de l'audit**, sélectionnez la case **Activer l'audit**.

Remarque
Si l'option est grisée, ceci signifie que vous n'avez pas l'autorisation de gérer l'audit. Vous devez être membre du groupe Sophos Console Administrators et disposer du droit d'**Audit** dans l'Enterprise Console pour activer ou désactiver l'audit. Retrouvez plus de renseignements sur les droits de l'utilisateur et sur l'administration déléguée dans l'*Aide de Sophos Enterprise Console*.

6 Autorisation d’accès aux données d’audit

Par défaut, seuls les administrateurs système ont accès aux données d’audit. Les autres utilisateurs ayant besoin d’accéder aux données pour créer des rapports d’audit doivent se voir explicitement accordé l’autorisation « Select » sur le schéma **Rapports** dans la base de données SophosSecurity. Vous pouvez effectuer l’opération à l’aide de l’utilitaire **sqlcmd** ou dans SQL Server Management Studio.

6.1 Autorisation d’accès aux données d’audit à l’aide de l’utilitaire sqlcmd

Pour autoriser l’accès aux données d’audit :

1. Copiez l’extrait de script ci-dessous dans un document (dans le Bloc-notes par exemple).

```
USE SophosSecurity;

DECLARE @stmt NVARCHAR(max);

DECLARE @Account VARCHAR(512)

/* Remplacez <Domaine>\<Utilisateur> par le nom du compte auquel vous
 voulez autoriser l’accès aux données d’audit. */

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. Remplacez les espaces réservés <Domaine> et <Utilisateur> dans la déclaration « SET @Account = N’<Domaine>\<Utilisateur>’ » par le nom de domaine et le nom d’utilisateur de l’utilisateur auquel vous souhaitez autoriser l’accès.

Si vos ordinateurs sont dans un groupe de travail, remplacez <Domaine> par le nom de l'ordinateur sur lequel la base de données est installée. Si l'utilisateur accède aux données à partir d'un groupe de travail différent, le compte de l'utilisateur doit exister sur les deux ordinateurs et avoir le même nom d'utilisateur et le même mot de passe.

3. Ouvrez l'Invite de commandes.
4. Connectez-vous à l'instance SQL Server. Saisissez :

```
sqlcmd -E -S <Serveur>\<Instance SQL Server>
```

L'instance par défaut de SQL Server est SOPHOS.

5. Copiez l'extrait du script à partir du fichier et collez-le dans l'Invite de commandes.
6. Appuyez sur Entrée pour exécuter le script.
Suite à l'exécution du script, l'utilisateur se voit accorder l'autorisation « Select » sur le schéma **Rapports** de la base de données SophosSecurity et peut accéder aux données d'audit.
7. Répétez la même procédure pour chaque utilisateur nécessitant l'accès.

6.2 Autorisation d'accès aux données d'audit à l'aide de SQL Server Management Studio

Avant de pouvoir accorder l'autorisation « Select » sur le schéma **Rapports** de la base de données SophosSecurity à un utilisateur de SQL Server Management Studio, veillez à ce que cet utilisateur dispose d'une connexion à SQL Server et qu'il est un utilisateur de la base de données SophosSecurity.

- Si l'utilisateur dispose déjà d'une connexion à SQL Server, ajoutez-le en tant qu'utilisateur de la base de données SophosSecurity. Dans l'Explorateur d'objets, développez le serveur, développez le dossier **Bases de données**, développez **SophosSecurity** et développez **Sécurité**. Cliquez avec le bouton droit de la souris sur **Utilisateurs** et cliquez sur **Nouvel utilisateur**. Dans la boîte de dialogue **Utilisateur de base de données**, saisissez le nom d'utilisateur et sélectionnez le nom de connexion. Cliquez sur **OK**.

  Retrouvez plus de renseignements sur la création d'utilisateurs de la base de données sur http://msdn.microsoft.com/fr-fr/library/aa337545.aspx#SSMSProcedure.

- Si l'utilisateur n'a pas de compte de connexion à SQL Server, ajoutez un nouveau compte de connexion à SQL Server en lui attribuant le rôle d'utilisateur de la base de données SophosSecurity. Dans l'Explorateur d'objets, développez le serveur, développez **Sécurité**. Cliquez avec le bouton droit de la souris sur **Connexions** et cliquez sur **Nouvelle connexion**. Dans la boîte de dialogue **Connexion**, sur la page **Général**, saisissez le compte ou le nom du groupe. Rendez-vous sur la page **Mappage de l'utilisateur** et sélectionnez **SophosSecurity**. Cliquez sur **OK**.

  Retrouvez plus de renseignements sur la création de connexions à SQL Server sur http://msdn.microsoft.com/fr-fr/library/aa337562.aspx#SSMSProcedure.

Pour autoriser l'accès d'un utilisateur aux données d'audit à l'aide de SQL Server Management Studio :

1. Dans l'Explorateur d'objets, développez le serveur, développez le dossier **Bases de données**, développez **SophosSecurity**, développez **Sécurité** et développez enfin **Schémas**.
2. Cliquez avec le bouton droit de la souris sur **Rapports** et cliquez sur **Propriétés**.
3. Dans la boîte de dialogue **Propriétés du schéma - Rapports**, sur la page des **Autorisations**, cliquez sur **Rechercher**. Dans la boîte de dialogue **Sélectionner des utilisateurs ou des rôles**, ajoutez un ou plusieurs utilisateurs.

4. Pour chaque utilisateur, dans la section **Autorisations pour <utilisateur>**, sur l'onglet **Explicite**, sélectionnez l'option **Sélectionner** sous **Accorder** et cliquez sur **OK**.

7 Création d’un rapport d’audit dans Microsoft Excel

Cet exemple vous montre comment importer des données d’audit de la base de données SQL Server et analyser ces données dans Microsoft Excel 2010.

Les sections suivantes vous expliquent comment créer un rapport d’audit dans Microsoft Excel en suivant les étapes principales suivantes :

- Connexion à la base de données d’audit (créer une nouvelle source de données).
- Créer une requête dans Microsoft Query.
- Renvoyer les données vers Excel.
- Créer un rapport dans Excel (un tableau ou un rapport de tableau croisé dynamique).

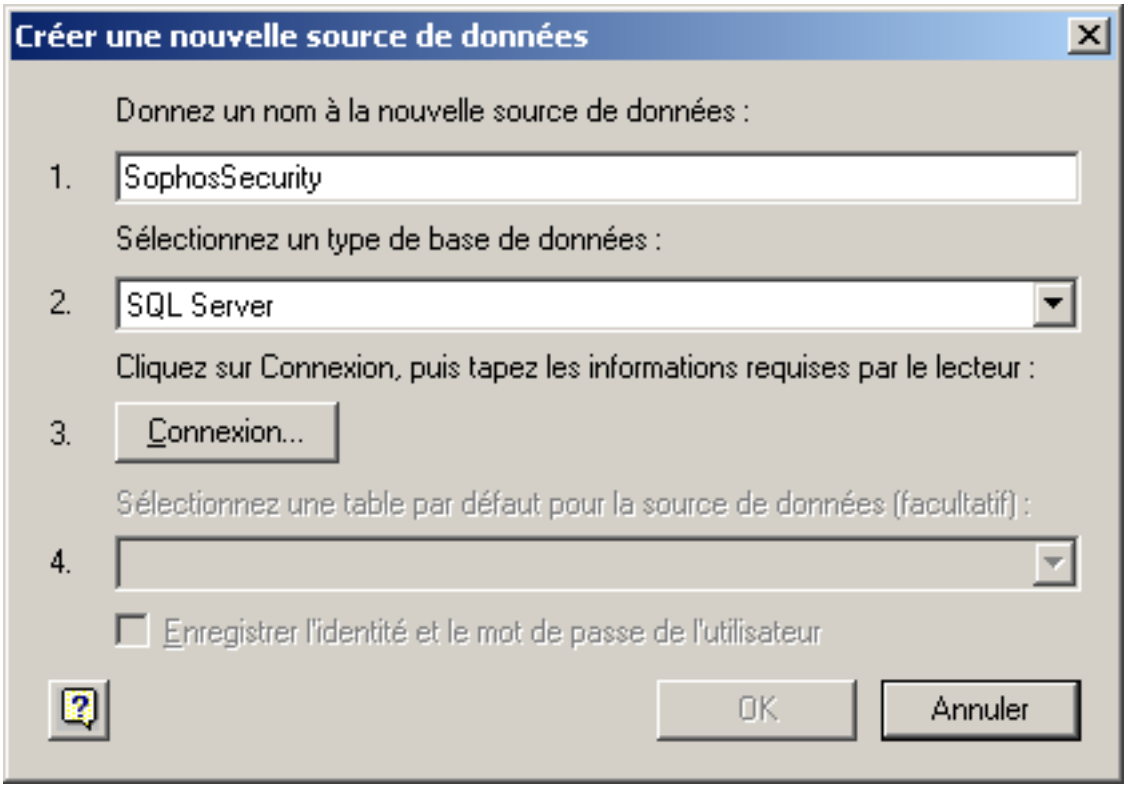
Remarque
Nous vous conseillons d’utiliser des ID numériques plutôt que des valeurs de chaînes si vous voulez relier toute logique externe aux données d’audit exportées. Par exemple, plutôt que d’utiliser les valeurs du champ **TargetType**, favorisez plutôt l’utilisation des valeurs du champ **TargetTypeId**. 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. Retrouvez un tableau des identifiants numériques (ID) dans l’Annexe : identifiants numériques (ID) des valeurs des champs de données (page 30) :

Retrouvez plus de renseignements sur l’importation de données SQL Server et sur la création de rapports Excel dans la documentation de Microsoft.

7.1 Connexion à la base de données

Vous devez d’abord vous connecter à la base de données.

1. Ouvrez Excel. Sur l’onglet **Données**, dans le groupe **Données externes**, cliquez sur **À partir d’autres sources** puis sur **Provenance : Microsoft Query**.
   La boîte de dialogue **Choisir une source de données** apparaît.
2. Dans l’onglet **Bases de données**, laissez **<Nouvelle source de données>** sélectionnée et cliquez sur OK.
3. Dans la boîte de dialogue **Créer une nouvelle source de données**, saisissez le nom que vous voulez donner à votre source de données. Dans cet exemple, nous allons utiliser **SophosAuditing**.
4. Dans le champ **Sélectionnez un type de base de données**, sélectionnez **SQL Server**.

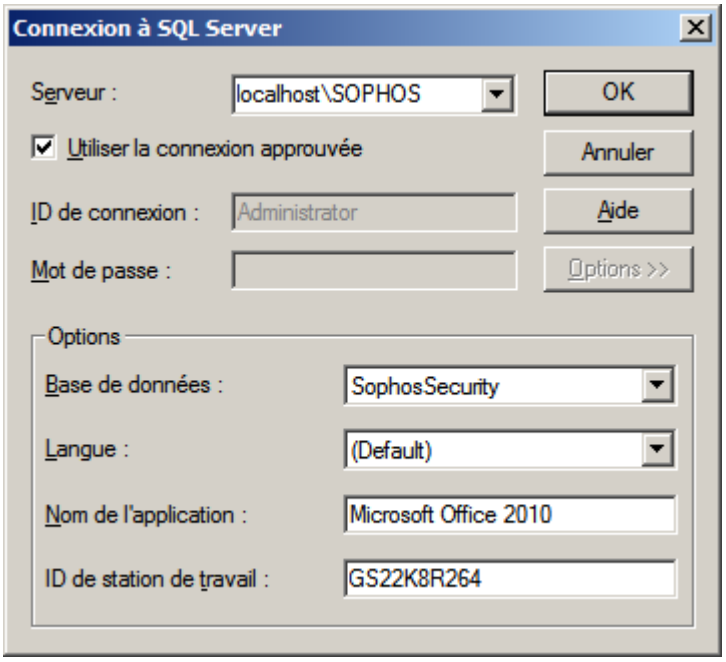


Cliquez sur **Connexion**.

5. Dans la boîte de dialogue **Connexion à SQL Server**, dans le champ **Serveur**, saisissez le nom du SQL Server auquel vous souhaitez vous connecter.

   Dans cet exemple, nous établissons la connexion à l'instance de la base de données SOPHOS sur le même ordinateur (localhost).

6. Cliquez sur **Options** pour développer le volet **Options**. Dans le champ **Base de données**, sélectionnez **SophosSecurity**.



Cliquez sur **OK**.

7. Dans la boîte de dialogue **Créer une nouvelle source de données**, sous **Sélectionnez une table par défaut pour la source de données (facultatif)**, sélectionnez **vAuditEventsAll**.

Cliquez sur **OK**.

7.2 Création d’une requête

Cet exemple vous indique comment faire une requête de la source de données que vous venez de créer afin d’obtenir des informations sur les stratégies de Contrôle des données ces trois derniers mois.

1. Dans la boîte de dialogue **Choisir une source de données**, dessélectionnez la case **Utiliser l’Assistant Requête pour créer et/ou modifier vos requêtes**.
2. Sélectionnez la source de données que vous avez créé aux étapes précédentes (dans cet exemple, **SophosAuditing**) et cliquez sur **OK**.
   La boîte de dialogue **Microsoft Query** affiche **Requête de SophosAuditing** avec le tableau par défaut **vAuditEventsAll**, que vous avez sélectionné lorsque vous avez créé la source de données.
3. Procédez de l’une des manières suivantes :
   - Créez une requête dans le Mode création.
     a) Dans la boîte de dialogue **Microsoft Query**, dans le menu **Critères**, cliquez sur **Ajouter des critères**.
     b) Dans la boîte de dialogue **Ajouter des critères**, près de **Champ**, sélectionnez **Horodateur**. Assurez-vous que le champ **Opérateur** est vide. Dans le champ **Valeur**, saisissez :

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

        Utilisez le séparateur de liste indiqué dans les paramètres Région et langue du Panneau de configuration. Par exemple, si votre séparateur de liste est un point-virgule, utilisez les points-virgules plutôt que les virgules dans l’instruction ci-dessus. Il se peut que vous receviez le message d'erreur « Extra ')' » si vous n’utilisez pas le bon séparateur de liste.

        Cliquez sur **Ajouter**. Le critère est ajouté à **Requête de SophosAuditing**.
     c) Dans la boîte de dialogue **Ajouter des critères** près de **Champ**, sélectionnez **TargetType**. Dans le champ **Opérateur**, sélectionnez **est égal à**. Dans le champ **Valeur**, sélectionnez ou saisissez **Stratégie**.

        Cliquez sur **Ajouter**. Le critère est ajouté à **Requête de SophosAuditing**.
     d) Dans la boîte de dialogue **Ajouter des critères** près de **Champ**, sélectionnez **TargetSubType**. Dans le champ **Opérateur**, sélectionnez **est égal à**. Dans le champ **Valeur**, sélectionnez ou saisissez **Contrôle de données**.

        Cliquez sur **Ajouter**. Le critère est ajouté à **Requête de SophosAuditing**.

        Dans la boîte de dialogue **Ajouter des critères**, cliquez sur **Fermer**.
     e) Dans la boîte de dialogue **Microsoft Query**, ajouter des champs à partir de **vAuditEventsAll** dans la requête en cliquant deux fois dessus. Vous pouvez également ajouter un champ à la requête en le faisant glisser du tableau vers la zone d’affichage.
   - Créez une requête dans le Mode SQL.

a) Dans **Microsoft Query**, cliquez sur le bouton **SQL** et saisissez votre instruction SQL, par exemple :

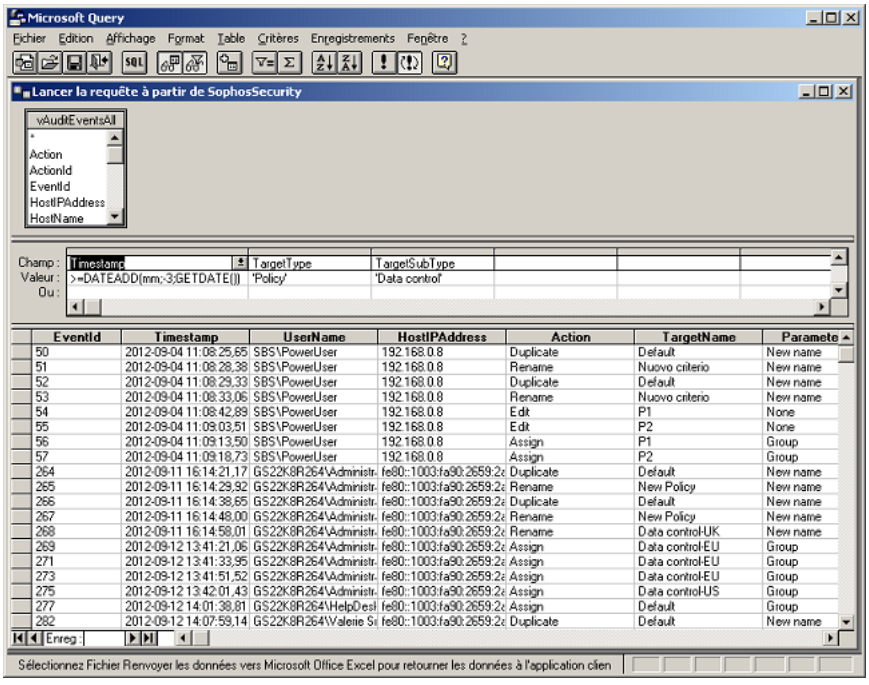
```
SELECT EventId, Timestamp, UserName, HostIPAddress, Action,
 TargetName, ParameterType, ParameterValue, Result

FROM SophosSecurity.Reports.vAuditEventsAll

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

ORDER BY EventId ASC
```

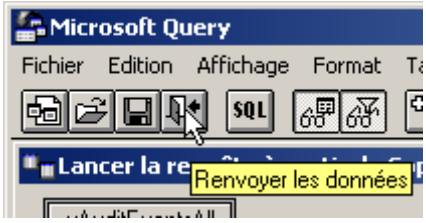
Cliquez sur **OK**.



4. Pour enregistrer la requête, dans le menu **Fichier**, cliquez sur **Enregistrer**.

7.3 Renvoi des données vers Excel

Pour renvoyer les données vers Excel, dans la boîte de dialogue **Microsoft Query**, cliquez sur le bouton **Renvoyer les données**.



Autrement, dans le menu **Fichier**, cliquez sur **Renvoyer les données vers Microsoft Excel**.

Retournez dans Excel, la boîte de dialogue **Importation de données** apparaît à partir de laquelle vous pouvez choisir le type de rapport à créer.

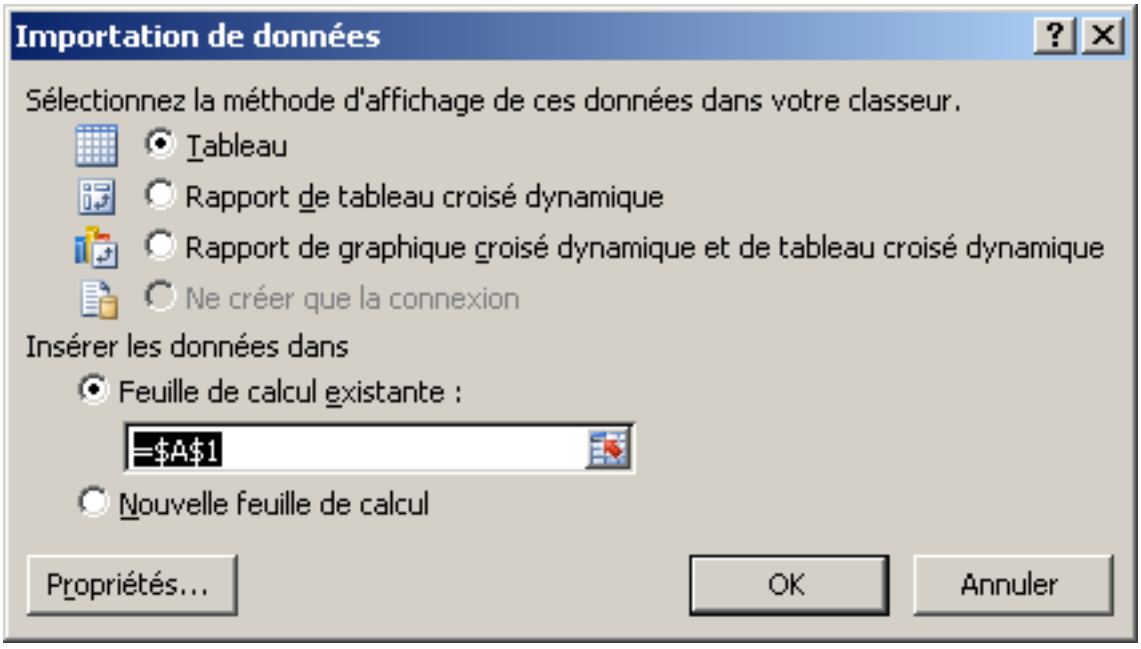
Les exemples suivants vous explique comment :

- Création d'un tableau (page 15)
- Création d'un rapport de tableau croisé dynamique (page 16)

7.4 Création d'un tableau

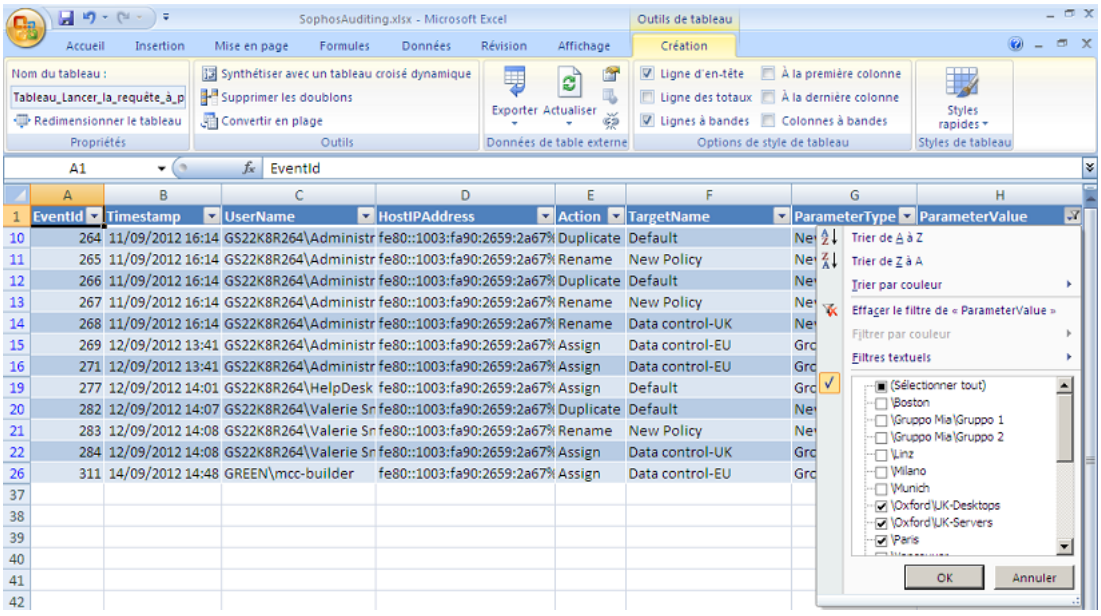
1. Si vous choisissez d'importer les données d'audit dans un tableau Excel, dans la boîte de dialogue **Importation de données**, sélectionnez **Tableau**.

   Pour placer les données dans la feuille de calcul existante en commençant par la cellule A1, laissez **Feuille de calcul existante** sélectionnée :

   Cliquez sur **OK**.

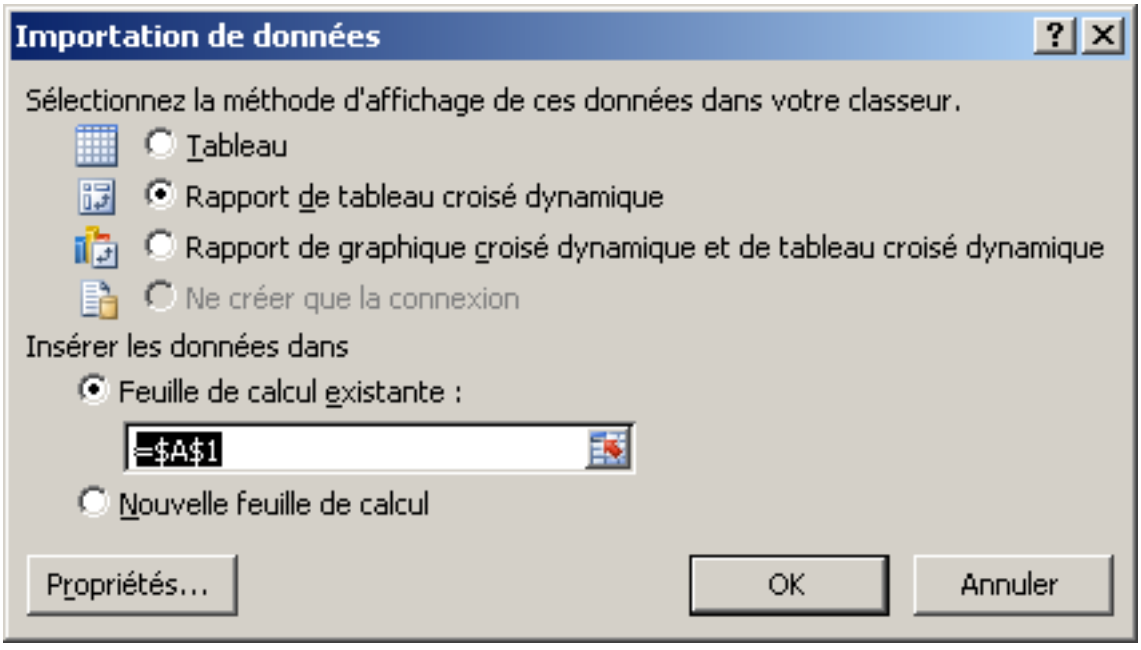
   Les données d'audit sont importées dans le tableau Excel.
2. Enregistrez votre classeur Excel.
3. Vous pouvez utiliser le filtre de recherche pour analyser vos données.



7.5 Création d'un rapport de tableau croisé dynamique

1. Si vous choisissez d'importer les données d'audit dans un tableau Excel, dans la boîte de dialogue **Importation de données**, sélectionnez **Rapport de tableau croisé dynamique**.

   Pour placer les données dans la feuille de calcul existante en commençant par la cellule A1, laissez **Feuille de calcul existante** sélectionnée :



   Cliquez sur **OK**.

   Le tableau de croisé dynamique vide apparaît dans la feuille de calcul.

2. Dans la **Liste de champs de tableau croisé dynamique** qui apparaît sur la droite, sélectionnez les champs que vous voulez voir.

Conseil
Vous pouvez filtrer les données avant d'ajouter les champs. Dans la **Liste de champs de tableau croisé dynamique**, allez dans la boîte **Choisissez les champs à ajouter au rapport :**, passez le pointeur de la souris au-dessus du nom du champ et cliquez sur la flèche du menu déroulant du filtre à côté du nom du champ. Dans le menu **Filtre**, sélectionnez les options de filtrage de votre choix.

3. Selon la façon dont vous souhaitez que votre tableau croisé dynamique apparaisse, faites glisser les champs entre les zones de la **Liste de champs de tableau croisé dynamique**. Par exemple, vous pouvez décider d'afficher les nom des utilisateurs et des stratégies qu'ils ont utilisé en tant que noms de ligne et les actions que les utilisateurs ont effectués sur les stratégies en tant que noms de colonne.
4. Pour filtrer le tableau croisé dynamique, sous **Outils de tableau croisé dynamique**, **Options**, cliquez sur **Insérer un segment**.
5. Dans la boîte de dialogue **Insérer des segments**, sélectionnez les segments que vous voulez utiliser et cliquez sur **OK**.

   Vous pouvez réorganiser les segments sur la feuille de calcul et la faire glisser à l'emplacement de votre choix. Vous pouvez également personnaliser vos segments en leur attribuant, par exemple, des couleurs. Pour cela, sélectionnez un segment. Sous **Outils de segment**, **Options**, sélectionnez l'un des **Styles de segment**.
6. Enregistrez votre classeur.

8 Exemples supplémentaires de création d'un rapport d'audit

Cette section vous indique comment créer une nouvelle requête à partir d'une source de données existante dans Microsoft Excel. Elle vous fournit également des exemples supplémentaires de requêtes que vous pouvez utiliser pour créer des rapports d'audit.

Cette section vous indique également comment créer un rapport contenant les détails sur les changements de stratégie au format XML.

8.1 Création d'une requête à partir d'une source de données existante

Pour créer un autre rapport d'audit à partir des source de données créées à la section Connexion à la base de données (page 11) :

1. Dans Excel, rendez-vous sur l'onglet **Données** et cliquez sur **À partir d'autres sources** puis cliquez sur **Provenance : Microsoft Query**.
2. Dans la boîte de dialogue **Choisir une source de données**, dessélectionnez la case **Utiliser l'Assistant Requête pour créer et/ou modifier vos requêtes**. Sélectionnez la source de données que vous avez créée auparavant (par exemple, SophosAuditing) et cliquez sur **OK**.
3. Dans **Microsoft Query**, cliquez sur le bouton **SQL** et saisissez une instruction SQL pour votre rapport.

La section suivante contient des exemples que vous pouvez utiliser.

8.2 Exemples supplémentaires de requêtes

Exemple 1 : quelles stratégies ont été changées par une personne définie au cours des 60 derniers jours

```
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
```

Remarque
Pour répertorier tous les champs que vous souhaitez inclure dans le rapport, saisissez « SELECT * » dans l'instruction afin de sélectionner tous les champs de la vue de la base de données.

Exemple 2 : quelles stratégies ont été appliquées à un groupe défini au cours des six derniers mois

```
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
```

Remarque
Si le groupe pour lequel vous créez un rapport est un sous-groupe d'un autre groupe, vous allez soit devoir saisir le chemin complet du groupe, soit utiliser l'instruction « se termine par » (à condition que le nom du groupe soit unique). Par exemple, pour créer un rapport pour le groupe \Lille\FR-Serveurs, vous pouvez soit saisir l'une des valeurs suivantes :

- `ParameterValue='\Lille\FR-Serveurs'`
- `ParameterValue Like '%FR-Serveurs'`

Exemple 3 : quels changements de groupe ont été effectués par une personne définie au cours des trois derniers mois

L'instruction suivante va générer un rapport indiquant les groupes qui ont été créés, supprimés, déplacés ou renommés ainsi que les ordinateurs que l'utilisateur a assigné à des groupes au cours des trois derniers mois.

```
SELECT *

FROM SophosSecurity.Reports.vAuditEventsAll

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

Exemple 4 : quels changements ont été effectués sur un groupe défini au cours des trois derniers mois

```
SELECT *

FROM SophosSecurity.Reports.vAuditEventsAll

WHERE (Timestamp>=DATEADD(mm,-3,GETUTCDATE()))
AND (ParameterValue='\Lille\FR-Ordinateurs')
```

8.3 Renvoi des données vers Excel

Après avoir créé une demande pour votre rapport d'audit, renvoyez les données dans Excel (**Fichier** > **Renvoyer les données vers Microsoft Excel**) et créez un rapport comme indiqué aux sections Création d'un tableau (page 15) et Création d'un rapport de tableau croisé dynamique (page 16).

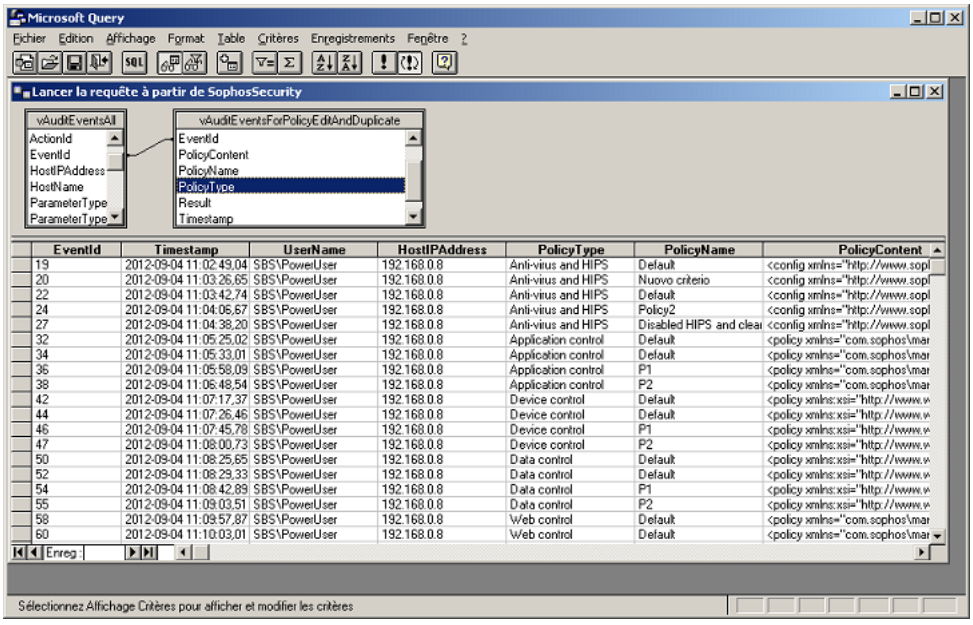
8.4 Création d'un rapport contenant les changements de la stratégie au format XML

Lorsqu'un utilisateur modifie une stratégie, les paramètres de cette stratégie sont enregistrés au format XML et sont accessibles via la vue de la base de données **Reports.vAuditEventsForPolicyEditAndDuplicate**.

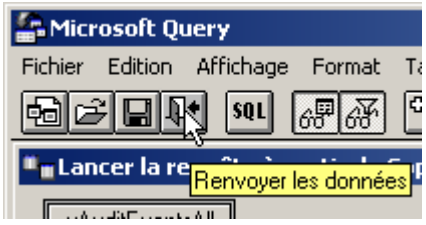
Vous pouvez créer un rapport contenant ces données supplémentaires en reliant les deux tableaux **Reports.vAuditEventsAll** et **Reports.vAuditEventsForPolicyEditAndDuplicate**.

1. Créez une nouvelle requête à partir d'une source de données existantes comme indiqué à la section Création d'une requête à partir d'une source de données existante (page 18).
2. Dans **Microsoft Query**, cliquez sur **Tableau** puis sur **Ajouter des tableaux**. Dans la boîte de dialogue **Ajouter des tableaux**, sélectionnez **vAuditEventsForPolicyEditAndDuplicate** et cliquez sur **Ajouter**. Dès que vous avez terminé, cliquez sur **Fermer**.
3. Reliez les tableaux en reliant les champs communs à ces deux tableaux. Cliquez sur le champ commun **EventID** dans le premier tableau et faites glisser la souris au-dessus du champ **EventID** dans le second tableau.
4. Ajoutez les champs à la requête en cliquant deux fois dessus. Vous pouvez également ajouter un champ à la requête en le faisant glisser du tableau vers la zone d'affichage.

Conseil
Vous pouvez utiliser la boîte de dialogue **Jointure** dans Microsoft Query (**Tableau** > **Jointure**) pour créer une requête reliant les deux tableaux.



5. Pour enregistrer la requête, dans le menu **Fichier**, cliquez sur **Enregistrer**.
6. Pour retourner dans Excel, cliquez sur le bouton **Renvoyer les données**.



Autrement, dans le menu **Fichier**, cliquez sur **Renvoyer les données vers Microsoft Excel**.

Retournez dans Excel, la boîte de dialogue **Importation de données** apparaît. Créez un tableau (voir la section Création d'un tableau (page 15)). La colonne **PolicyContent** contient les changements de la configuration de la stratégie au format XML.

Conseil

Si vous utilisez Microsoft SQL Server Management Studio, vous pouvez demander directement la vue **Reports.vAuditEventsForPolicyEditAndDuplicate**. Lorsque vous allez suivre le lien dans la colonne **PolicyContent** des résultats de la requête, le contenu de la stratégie sera affiché dans un éditeur XML sous un format plus facile à lire que dans un tableur Excel.

9 Quelles actions sont soumises à l’audit ?

Les catégories d’actions soumises à l’audit incluent :

- Actions de l’ordinateur
- Gestion de groupes d’ordinateurs
- Gestion des stratégies
- Gestion des rôles
- Gestion de Sophos Update Manager
- Événements système

9.1 Actions de l’ordinateur

Les actions de l’ordinateur suivantes sont soumises à l’audit :

- Approuver/résoudre les alertes et les erreurs
- Protéger un ordinateur
- Mettre à jour un ordinateur
- Supprimer un ordinateur
- Effectuer le contrôle intégral du système d’un ordinateur

9.2 Gestion de groupes d’ordinateurs

Les actions consignées pour la gestion de groupes d’ordinateurs sont :

- Créer un groupe
- Supprimer un groupe
- Déplacer un groupe
- Renommer un groupe
- Assigner un ordinateur à un groupe

9.3 Gestion des stratégies

Les actions consignées pour la gestion des stratégies sont :

- Création d’une stratégie (page 23)
- Renommer une stratégie
- Duplication d’une stratégie (page 23)
- Modifier une stratégie
- Assigner une stratégie à un ordinateur

- Rétablir les paramètres par défaut de la stratégie
- Suppression d'une stratégie (page 23)

9.3.1 Création d'une stratégie

Lorsque vous créez une nouvelle stratégie, la stratégie par défaut est dupliquée et apparaît sous le nom « Nouvelle stratégie ». Vous pouvez renommer la nouvelle stratégie immédiatement après sa création. Par exemple, si vous créez une nouvelle stratégie Antivirus et HIPS et la renommer « Serveurs », les entrées d'audit suivantes vont être créées :

Tableau 1 : création d'une nouvelle stratégie et attribution d'un nom

Action	Type de cible	Sous-type de cible	Nom de la cible	Type de paramètre	Valeur du paramètre	Résultat
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 Duplication d'une stratégie

Lorsque vous dupliquez une stratégie, un événement « Dupliquer une stratégie » est créé. Par exemple :

Tableau 2 : Duplication d'une stratégie

Action	Type de cible	Sous-type de cible	Nom de la cible	Type de paramètre	Valeur du paramètre	Résultat
Duplicate	Policy	Web Control	TestPolicy1	New name	Copy of TestPolicy1	Success

9.3.3 Suppression d'une stratégie

Lorsque vous supprimez une stratégie, tous les groupes utilisant la stratégie supprimée utiliseront dorénavant la stratégie par défaut. Dans ce cas de figure, aucun événement d'audit séparé n'est créé qui indique que la stratégie par défaut a été réappliquée.

9.4 Gestion des rôles

Les actions consignées pour la gestion des rôles sont :

- Créer un rôle
- Supprimer un rôle
- Renommer un rôle

- Dupliquer un rôle
- Ajouter un utilisateur à un rôle
- Supprimer un utilisateur d'un rôle
- Ajouter un droit à un rôle
- Supprimer un droit d'un rôle

9.5 Gestion de Sophos Update Manager

Les actions consignées pour la gestion de Sophos Update Manager sont :

- Mettre à jour un gestionnaire de mise à jour
- Mettre un gestionnaire de mise à jour en conformité avec la configuration
- Approuver une alerte
- Supprimer un gestionnaire de mise à jour
- Configurer un gestionnaire de mise à jour

9.5.1 Comment les changements de configuration du gestionnaire de mise à jour sont enregistrés ?

Dans l'Enterprise Console, la boîte de dialogue **Configuration du gestionnaire de mise à jour** contient de nombreux onglets et d'options de configuration qui composent essentiellement les stratégies de configuration du gestionnaire de mise à jour. Lorsque vous modifiez la configuration du gestionnaire de mise à jour, les actions effectuées sur les stratégies suivantes sont journalisées :

- **Update Manager - subscription** : indique les abonnements logiciel maintenus à jour par le gestionnaire de mise à jour.
- **Update Manager - upstream** : indique la source de mise à jour du gestionnaire de mise à jour.
- **Update Manager - downstream** : indique les partages dans lesquels le gestionnaire de mise à jour télécharge les logiciels.
- **Update Manager - schedule** : indique la fréquence à laquelle le gestionnaire de mise à jour vérifie la présence de nouvelles données de détection des menaces et de mises à jour de logiciels.
- **Update Manager - general** : indique les options de journalisation du gestionnaire de mise à jour.
- **Software subscription** : indique la configuration d'un abonnement logiciels, par exemple, « Recommended ».

Il arrive parfois que les changements d'une stratégie du gestionnaire de mise à jour entraînent des changements des stratégies des autres gestionnaires de mise à jour (tels que les changements de la valeur d'un identifiant de paramètre). Dans certains cas, vous pouvez observer plusieurs enregistrements dans la base de données SophosSecurity correspondant à un changement que vous avez effectué. Par exemple, si vous créez une planification sur l'onglet **Planification** de la boîte de dialogue **Configuration du gestionnaire de mise à jour** et cliquez sur OK. Les entrées d'audit suivantes vont être créées :

Tableau 3 : création d'une planification de mise à jour du gestionnaire de mise à jour

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 - subscriptio n		None		Success

Dans ce cas, seule la première action, consignée pour la stratégie **Update Manager - schedule** aboutira à un changement effectif de la configuration. Le reste des changements de la stratégie consignée pour cet événement sont des changements d'identifiants de paramètres internes. Pour vérifier quelles modifications ont été apportées, vous pouvez utiliser la vue **Reports.vAuditEventsForPolicyEditAndDuplicate** de la base de données SophosSecurity comme indiqué à la section Création d'un rapport contenant les changements de la stratégie au format XML (page 20).

9.6 Événements système

Les événements système suivants sont soumis à l'audit :

- Activation de la fonction d'audit
- Désactivation de la fonction d'audit

10 Champs de données de Sophos Auditing

Les vues ci-dessous de la base de données ou des sources de données sont disponibles pour Sophos Auditing :

- Reports.vAuditEventsAll
- Reports.vAuditEventsForPolicyEditAndDuplicate

Les champs de données disponibles pour chacune de ces sources de données sont indiqués ci-dessous. 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). Les champs communs aux deux vues apparaissent en caractères gras.

Reports.vAuditEventsAll

La vue de la base de données **Reports.vAuditEventsAll** contient la liste complète des événements d'audit et la majorité des informations d'audit.

Champ de données	Type de données	Description
EventId	integer	Un identifiant numérique (ID) exclusif à l'événement.
Timestamp	datetime	L'heure à laquelle l'action consignée dans l'événement a eu lieu.
Action	nvarchar(128)	L'action consignée dans l'événement, par exemple, Create, Edit, Rename, Assign, Delete.
TargetType	nvarchar(128)	Le type d'objet ou de paramètre de configuration modifié par l'action. Par exemple, Group, Computer, Policy, Role.
TargetSubType	nvarchar(128)	Le sous-type d'objet ou de paramètre modifié par l'action, partout ou ceci est applicable. Par exemple, le nom de la stratégie modifiée, telle que Anti-virus and HIPS ou Data control.
TargetName	nvarchar(4000)	Le nom de l'objet ou du paramètre modifié par l'action. Par exemple, le nom de la stratégie ou du groupe défini par l'utilisateur.
ParameterType	nvarchar(128)	Le type de nouveau paramètre ou d'objet assigné à la cible. Par exemple, pour Action="Rename" et TargetType="Policy", ParameterType="New name". Pour Action="Assign" et TargetType="Computer", ParameterType="Group".

Champ de données	Type de données	Description
ParameterValue	nvarchar(4000)	La valeur du nouveau paramètre ou du nouvel objet. Par exemple, le nom de la nouvelle stratégie définie par l'utilisateur ou du nouveau groupe auquel l'ordinateur a été assigné.
Result	nvarchar(128)	Le succès ou l'échec de l'action est indiqué par la valeur « Success » ou « Failure ».
UserName	nvarchar(256)	Le nom de l'utilisateur qui a effectué l'action.
HostName	nvarchar(256)	Le nom de l'ordinateur à partir duquel l'utilisateur a effectué l'action.
HostIPAddress	nvarchar(48)	L'adresse IP de l'ordinateur à partir duquel l'utilisateur a effectué l'action. Si les connexions réseau entre le serveur et l'Enterprise Console sont établies via IPv6, les adresses IPv6 seront enregistrées. Autrement, les adresses IPv4 seront enregistrées.
ActionId	integer	Un identifiant numérique (ID) exclusif à l'action.
TargetTypeId	integer	Un identifiant numérique (ID) exclusif au type de cible.
TargetSubTypeId	integer	Un identifiant numérique (ID) exclusif au sous-type de cible.
ParameterTypeId	integer	Un identifiant numérique (ID) exclusif au type de paramètre.
SubEstateId	integer	Un identifiant numérique (ID) exclusif au sous-parc de l'utilisateur.
ResultId	integer	Un identifiant numérique (ID) exclusif au résultat, 1 (succès) ou 0 (échec).
UserSid	nvarchar(128)	L'identifiant de sécurité de l'utilisateur. .

Reports.vAuditEventsForPolicyEditAndDuplicate

La vue de la base de données **Reports.vAuditEventsForPolicyEditAndDuplicate** contient des informations sur les changements de stratégie.

Champ de données	Type de données	Description
EventId	integer	Un identifiant numérique (ID) exclusif à l'événement.

Champ de données	Type de données	Description
Timestamp	datetime	L'heure à laquelle l'action consignée dans l'événement a eu lieu.
Action	nvarchar(128)	L'action consignée dans l'événement.
Result	nvarchar(128)	Le succès ou l'échec de l'action est indiqué par la valeur « Success » ou « Failure ».
PolicyType	nvarchar(128)	Le type de stratégie modifié par l'action. Par exemple, Anti-virus and HIPS ou Web control.
PolicyName	nvarchar(4000)	Le nom que l'utilisateur a donné à la stratégie.
PolicyContent	XML	L'extrait des modifications de la configuration de la stratégie au format XML.
UserName	nvarchar(256)	Le nom de l'utilisateur qui a effectué l'action.

11 Résolution des problèmes

En cas d’échec de Sophos Auditing, un événement est consigné dans le journal des événements des applications Windows avec la source « Sophos Auditing ». Ceci arrive généralement en cas de problème de connectivité de la base de données.

12 Annexe : identifiants numériques (ID) des valeurs des champs de données

Les tableaux suivants vous indiquent les identifiants numériques exclusifs à certaines valeurs de champs de données de Sophos Auditing.

Nous vous conseillons d'utiliser ces ID numériques plutôt que des valeurs de chaînes si vous voulez relier toute logique externe aux données d'audit exportées. 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.

Champ de données	Valeur du champ de données	Identifiant numérique
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
	Comply	17

Champ de données	Valeur du champ de données	Identifiant numérique
TargetTyp e	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
	Tamper protection	19
	Web control	22
	Exploit prevention	30
TargetSubType for TargetType=Configuration	Unknown	0
	Dashboard	1
	Email alerts	2
	Purge	3
	Audit	4

Champ de données	Valeur du champ de données	Identifiant numérique
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 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.

14 Mentions légales