SOPHOS

Security made simple.

Sophos Enterprise Console
Guida per utenti sulla funzione di Controllo

Versione prodotto: 5.5

Sommario

1 Informazioni sulla guida....3
2 Sophos Auditing....4
3 Passaggi chiave per l'utilizzo di Sophos Auditing....5
4 Verifica che il database sia protetto....6
4.1 Protezione del databse incorporata....6
4.2 Protezione dei database migliorata....6
5 Abilitazione di Sophos Auditing....8
6 Concessione di accesso ai dati di controllo....9
6.1 Concessione di accesso ai dati di controllo tramite utilità sqlcmd....9
6.2 Concessione di accesso ai dati di controllo tramite SQL Server Management Studio....10
7 Creazione di un report di controllo in Microsoft Excel....12
7.1 Impostazione di una connessione al database....12
7.2 Creazione di una query....14
7.3 Restituzione dei dati a Excel....16
7.4 Creazione di una tabella....16
7.5 Creazione report Tabella pivot....17
8 Ulteriori esempi sulla creazione di un report di controllo....19
8.1 Creazione di una query da una fonte dei dati esistente....19
8.2 Ulteriori esempi di query....19
8.3 Restituzione dei dati a Excel....21
8.4 Creazione di un report contenente le modifiche ai criteri in formato XML....21
9 Azioni sottoposte a controllo....23
9.1 Azioni del computer....23
9.2 Gestione di gruppi di computer....23
9.3 Gestione criteri....23
9.4 Gestione dei ruoli....24
9.5 Gestione di Sophos Update Manager....25
9.6 Eventi di sistema....26
10 Campi dati di Sophos Auditing....27
11 Risoluzione dei problemi....30
12 Appendice: ID numerici dei valori del campo dati....31
13 Supporto tecnico....34
14 Note legali....35

1 Informazioni sulla guida

Questa guida indica come utilizzare la funzione di controllo in Sophos Enterprise Console per monitorare le modifiche apportate alla configurazione di Enterprise Console e altre azioni eseguite da utenti o sistemi. È stata scritta per amministratori di sistema e di database.

Si basa sul presupposto che si conosca e si stia già utilizzando Sophos Enterprise Console (SEC).

La documentazione Sophos è reperibile online alla pagina web: http://www.sophos.com/it-it/support/documentation.

2 Sophos Auditing

Sophos Auditing consente di monitorare le modifiche apportate alla configurazione di Enterprise Console, oltre che altre azioni eseguite da utenti o sistemi. Queste informazioni sono utili per la conformità alle normative e la risoluzione dei problemi, oppure, in caso di attività malevoli, per azioni di analisi e indagine.

Per impostazione predefinita, il controllo è disabilitato. Dopo avere abilitato il controllo in Enterprise Console, nel database di SQL Server, SophosSecurity, verrà aggiunta una voce di controllo ogni qualvolta determinate impostazioni di configurazioni vengano modificate o azioni specifiche vengano eseguite.

Tale voce di controllo includerà le seguenti informazioni:

- Azione eseguita
- Utente che ha eseguito l'azione
- Computer dell'utente
- Sottoambiente dell'utente
- Data e ora dell'azione

Vengono sottoposte a controllo sia le azioni che hanno esito positivo sia quelle con esito negativo; in questo modo le voci di controllo potranno mostrare chi ha eseguito in modo efficace determinate azioni all'interno del sistema e chi ne ha intraprese altre che non hanno invece avuto successo.

È possibile utilizzare programmi prodotti da terzi, quali Microsoft Excel, Microsoft Access, Microsoft SQL Server Reporting Services o Crystal Reports, per accedere e analizzare i dati archiviati nel database di controllo.

Importante: Sophos Auditing rende i propri dati disponibili anche ad applicazioni prodotte da terzi. Utilizzando questa funzione ci si assume la responsabilità della sicurezza dei dati resi accessibili; ciò significa accertarsi che solo utenti autorizzati possano accedere a tali dati. Per considerazioni sulla sicurezza, vedere la sezione Verifica che il database sia protetto a pagina 6.

Per maggiori informazioni su quali siano le azioni sottoposte a controllo, consultare la sezione Azioni sottoposte a controllo a pagina 23.

3 Passaggi chiave per l'utilizzo di Sophos Auditing

I passaggi chiave per l'utilizzo di Sophos Auditing sono:

- Verificare che il database sia sicuro
- Abilitare la funzione di controllo.
- Concessione di accesso ai dati di controllo
- Creare un report di controllo

4 Verifica che il database sia protetto

4.1 Protezione del databse incorporata

Enterprise Console e il database SophosSecurity mettono a disposizione dei dati di controllo numerose opzioni di protezione incorporate:

- Access Control
- Blocco rimozione

Access Control

Access Control viene implementato ai seguenti livelli:

- Interfaccia utente grafica (GUI) front-end

  Solo gli utenti in possesso del diritto di **Controllo** in Enterprise Console e membri del gruppo Sophos Console Administrators possono abilitare o disabilitare il controllo.

- Database

  Per impostazione predefinita, solo gli utenti membri del gruppo Sophos DB Admins possono accedere alle interfacce del database. Inoltre, le procedure di archiviazione dalle interfacce del database richiedono la presentazione di un token della sessione utente valido. Tale token viene generato dal sistema al momento dell'apertura della GUI da parete di un utente, oppure quando un utente apporta modifiche al sottoambiente.

Blocco rimozione

Il database è progettato in modo tale che i dati dell'evento di controllo non possano essere alterati. Non è necessario aggiornare i dati nel database di controllo, eccezion fatta per determinate impostazioni di configurazione. Sono presenti trigger che eseguiranno il rollback di qualsiasi tentativo di aggiornamento o cancellazione dei dati dalle tabelle.

I dati potranno essere cancellati solo eliminando il database. I dati che risalgono a due anni prima vengono cancellati automaticamente, come parte della procedura standard di cancellazione pianificata nel server di Enterprise Console. Per cancellare i dati è anche possibile utilizzare il tool PurgeDB (vedere http://www.sophos.com/it-it/support/knowledgebase/109884.aspx).

4.2 Protezione dei database migliorata

Controllo del database

Oltre alla protezione dei database di Enterprise Console, si consiglia un'ulteriore protezione al livello dell'istanza di SQL Server (se non ancora applicata), in modo tale da controllare l'attività degli utenti e le modifiche apportate in SQL Server.

Per esempio, se si esegue l'edizione di Enterprise del server SQL 2008, è possibile utilizzare la funzione di controllo di SQL Server. Le versioni precedenti di SQL Server potranno supportare il controllo accessi, il controllo basato su trigger, oltre che il controllo eventi grazie alla funzionalità di traccia incorporata.

Per ulteriori informazioni sulle funzionalità a disposizione per intraprendere operazioni di controllo, oltre che sulle modifiche al sistema SQL Server, consultare la documentazione relativa alla versione in uso di SQL Server. Per esempio:

- SQL Server Audit (Database Engine)
- Controllo (Motore di database), SQL Server 2008 R2
- Auditing in SQL Server 2008
- Controllo (Motore di database), SQL Server 2008

Connessioni di cifratura del database

Si consiglia caldamente la cifratura di tutte le connessioni fra 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)
- Connessioni cifrate a SQL Server 2008 R2
- Come abilitare la cifratura SSL per un'istanza di SQL Server utilizzando Microsoft Management Console

Controllo dell'accesso ai backup del database

Verificare che un controllo dell'accesso restrittivo venga applicato in modo adeguato a tutti i backup o copie del database. Ciò consentirà di evitare che utenti non autorizzati accedano a file, li modifichino, o cancellino inavvertitamente.

Nota: I link presenti in questa sezione si riferiscono a informazioni aggiornate da terzi e sono stati inclusi come ulteriore riferimento per gli utenti. Nonostante l'impegno costante nel verificare l'accuratezza dei link citati nella documentazione, tali link potrebbero essere modificati a insaputa di Sophos.

5 Abilitazione di Sophos Auditing

Per impostazione predefinita, il controllo è disabilitato. Per abilitare l controllo:

1. In Enterprise Console, nel menu **Strumenti**, cliccare su **Gestisci controllo**.
2. Nella finestra **Gestisci controllo**, selezionare la casella di spunta **Abilita il controllo**.

   Nota: Se l'opzione non è selezionabile, non si è in possesso dei diritti necessari per la gestione del controllo. È necessario essere membri del gruppo Sophos Console Administrators e disporre del diritto di **Controllo** in Enterprise Console per poter abilitare o disabilitare tale funzione. Per informazioni sui diritti degli utenti e sull'amministrazione basata sui ruoli, consultare la *Guida in linea di Sophos Enterprise Console*.

6 Concessione di accesso ai dati di controllo

Per impostazione predefinita, solo gli amministratori di sistema possono accedere ai dati di controllo. Tutti gli altri utenti che devono poter accedere a tali dati per creare report di controllo dovranno ricevere autorizzazione "Select" nello schema **Reports** del database SophosSecurity. Ciò può essere eseguito tramite utilità **sqlcmd** o in SQL Server Management Studio.

6.1 Concessione di accesso ai dati di controllo tramite utilità sqlcmd

Per concedere accesso ai dati di controllo:

1. Copiare il seguente frammento di script in un documento, per esempio in un file del Blocco note.

```
USE SophosSecurity;

DECLARE @stmt NVARCHAR(max);

DECLARE @Account VARCHAR(512)

/* Sostituire <Domain>\<User> col nome dell'account a cui concedere
 accesso ai dati di controllo. */

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. Sostituire i segnaposto <Domain> e <User> utilizzati in "SET @Account = N'<Domain>\<User>'" con dominio e nome utente a cui concedere accesso ai dati di controllo.

   Se i computer appartengono a un gruppo di lavoro, sostituire la dicitura <Domain> con il nome del computer in cui è installato il database. Se l'utente accederà ai dati da un computer del gruppo di lavoro differente, l'account utente dovrà esistere in entrambi i computer, con lo stesso nome utente e password.

3. Aprire il prompt dei comandi.
4. Connettersi all'istanza di SQL Server. Digitare:

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

   L'istanza predefinita del server SQL è SOPHOS.

5. Copiare il frammento di script dal file e incollarlo nel prompt di comando.
6. Premere Invio per eseguire lo script.

   Una volta eseguito lo script, all'utente è concessa l'autorizzazione "Select" nello schema **Reports** del database SophosSecurity e può quindi accedere ai dati di controllo.

7. Ripetere questa procedura per tutti gli utenti a cui si desidera autorizzare l'accesso.

6.2 Concessione di accesso ai dati di controllo tramite SQL Server Management Studio

Prima di attribuire autorizzazione "Select" nello schema **Report** del database SophosSecurity a un utente in SQL Server Management Studio, verificare che l'utente possieda un account di accesso di SQL Server e sia utente del database SophosSecurity.

- Se l'utente è già in possesso di un account di accesso di SQL Server, aggiungerlo come utente del database SophosSecurity. In Esplora oggetti, espandere il server, espandere la cartella **Database**, espandere **SophosSecurity** e quindi espandere **Protezione**. Cliccare col taso destro del mouse su **Utenti** quindi cliccare su **Nuovo utente**. Nella finestra di dialogo **Utente database**, inserire il nome utente e selezionare il nome accesso. Cliccare su **OK**.

  Per maggiori informazioni sulla creazione di utenti del database, vedere http://msdn.microsoft.com/it-it/library/aa337545.aspx#SSMSProcedure.

- Se l'utente non dispone di un account di accesso di SQL Server, aggiungerne uno e abilitarlo come utente del database SophosSecurity. In "Esplora oggetti", espandere il server, e quindi **Protezione**. Cliccare col taso destro del mouse su **Accessi** quindi cliccare su **Nuovo account accesso**. Nella finestra di dialogo **Accesso**, nella pagina **Generale**, inserire il nome dell'account o gruppo. Andare alla pagina **Mapping utenti** e selezionare **SophosSecurity**. Cliccare su **OK**.

  Per maggiori informazioni sulla creazione di account di accesso di SQL Server, vedere http://msdn.microsoft.com/it-it/library/aa337562.aspx#SSMSProcedure.

Per concedere a un utente accesso ai dati di controllo in SQL Server Management Studio:

1. In Esplora oggetti, espandere il server, espandere la cartella **Database**, espandere **SophosSecurity**, quindi espandere **Protezione**, e infine espandere anche **Schemi**.
2. Cliccare col tasto destro del mouse su **Report** e quindi cliccare su **Proprietà**.

3. Nella finestra di dialogo **Proprietà schema - report**, nella pagina **Autorizzazioni**, cliccare su **Cerca**. Nella finestra di dialogo **Selezione utenti o ruoli**, aggingere uno o più utenti.
4. Per ciascun utente, nella sezione **Autorizzazioni per <utente>**, nella scheda **Esplicito**, scegliere **Seleziona** sotto **Concedi**, quindi cliccare su **OK**.

7 Creazione di un report di controllo in Microsoft Excel

In questo esempio si mostra come importare i dati di controllo dal database di SQL Server e analizzarli in Microsoft Excel 2010.

Le seguenti sezioni descrivono come generare un report di controllo in Microsoft Excel eseguendo i seguenti passaggi chiave:

- Impostare un collegamento con il database di controllo (creare una fonte dei dati).
- Creare una query in Microsoft Query.
- Restituire i dati a Excel.
- Creare un report in Excel (una tabella o un report di tabella pivot).

Nota: Si consiglia l'utilizzo di ID numeriche piuttosto che valori stringa, se si desidera attribuire un ordine logico ai dati di controllo esportati. Per esempio, invece che utilizzare valori provenienti dal campo **TargetType**, utilizzare invece quelli del campo **TargetTypeId**. Ciò può evitare problemi di compatibilità nel caso valori stringa vengano modificati nei rilasci futuri di Enterprise Console. Per una tabella degli ID numerici, vedere l'Appendice: ID numerici dei valori del campo dati a pagina 31.

Per ulteriori informazioni sull'importazione dei dati di SQL Server e la creazione di report in Excel, consultare la documentazione Microsoft.

7.1 Impostazione di una connessione al database

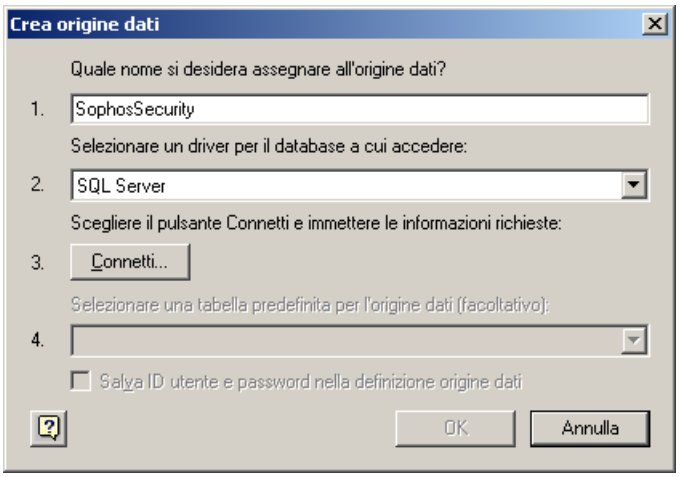
Per prima cosa, connettersi al database.

1. Aprire Excel. Nella scheda **Dati**, all'interno del gruppo **Recupera dati esterni**, cliccare su **Da altre origini**, e quindi su **Da Microsoft Query**.

   Viene visualizzata la finestra di dialogo **Scegli origine dati**.

2. Nella scheda **Database**, lasciare selezionato **<nuova origine database>** e cliccare su OK.
3. Nella finestra di dialogo **Crea nuova origine dati**, digitare il nome che si desidera attribuire alla nuova fonte dei dati. In questo esempio il nome scelto è **SophosAuditing**.

4. Nella casella **Selezionare un driver relativo al tipo di database a cui si desidera accedere**, scegliere **SQL Server**.

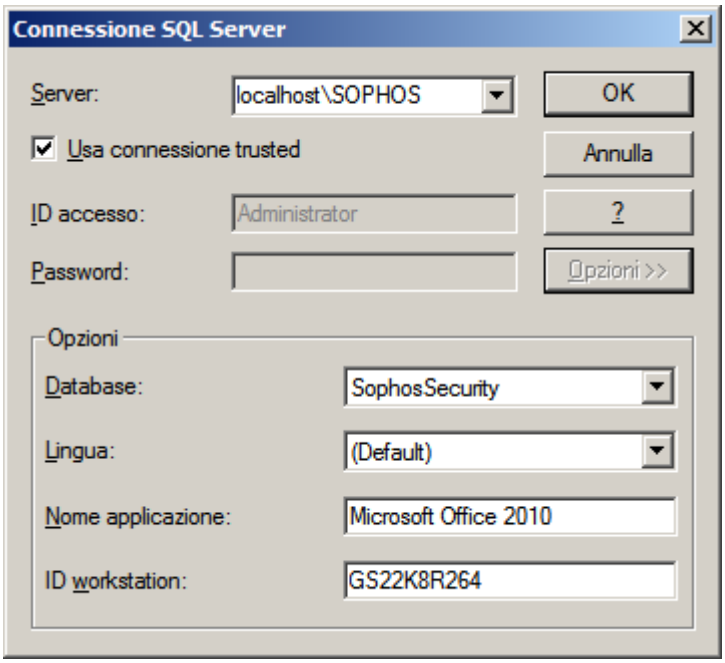


   Cliccare su **Connetti**.

5. Nella finestra di dialogo di **Connessione SQL Server**, nella casella **Server**, inserire il nome dell'SQL Server a cui ci si desidera connettere.

   In questo esempio ci si sta connettendo all'istanza del database SOPHOS nello stesso computer (localhost).

6. Cliccare su **Opzioni** per espandere il pannello **Opzioni**. Nella casella **Database**, selezionare **SophosSecurity**.



   Cliccare su **OK**.

7. Nella finestra di dialogo **Crea nuova origine dati**, sotto **una tabella predefinita per l'origine dati (opzionale)**, selezionare **vAuditEventsAll**.

   Cliccare su **OK**.

7.2 Creazione di una query

Questo esempio mostra come effettuare una query alla fonte dei dati appena creata, per ottenere informazioni sulle modifiche apportate ai criteri di Data Control negli ultimi tre mesi.

1. Nella finestra di dialogo **Scegli origine dati**, deselezionare la casella di spunta **Usa Creazione guidata Query per creare/modificare query**.
2. Selezionare la fonte dei dati creata nei passaggi precedenti (in questo esempio **SophosAuditing**) e cliccare su **OK**.

   La finestra di dialogo **Microsoft Query** visualizza la dicitura **Query da SophosAuditing** con la tabella predefinita, **vAuditEventsAll**, selezionata al momento della creazione della fonte dei dati.

3. Effettuare una delle seguenti operazioni:
   - Creare una query in Visualizzazione struttura.
     1. Nella finestra di dialogo **Microsoft Query**, nel menu **Criteri**, cliccare su **Aggiungi criteri**.
     2. Nella finestra di dialogo **Aggiungi criteri**, di fianco a **Campo**, selezionare **Timestamp**. Verificare che il campo **Operatore** sia vuoto. Nel campo **Valore**, digitare:

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

        Utilizzare il separatore di elenco specificato nelle impostazioni dell'opzione Paese e lingua del Pannello di controllo. Per esempio, se il separatore di elenco è un punto e virgola, nella dichiarazione qui sopra sostituire le virgole con punti e virgola . Si potrebbe ricevere il messaggio di errore "Extra ')'", nel caso sia stato scelto un separatore di elenco errato.

        Cliccare su **Aggiungi**. Il criterio vine aggiunto a **Query da SophosAuditing**.

     3. Nella finestra di dialogo **Aggiungi criteri**, di fianco a **Campo**, selezionare **TargetType**. Nel campo **Operatore**, selezionare **uguale a**. Nel campo **Valore**, selezionare o digitare **Criterio**.

        Cliccare su **Aggiungi**. Il criterio vine aggiunto a **Query da SophosAuditing**.

     4. Nella finestra di dialogo **Aggiungi criteri**, di fianco a **Campo**, selezionare **TargetSubType**. Nel campo **Operatore**, selezionare **uguale a**. Nel campo **Valore** selezionare o digitare **Controllo dati**.

        Cliccare su **Aggiungi**. Il criterio vine aggiunto a **Query da SophosAuditing**.

        Nella finestra di dialogo **Aggiungi criteri**, cliccare su **Chiudi**.

     5. Nella finestra di dialogo **Microsoft Query**, aggiungere campi da **vAuditEventsAll** alla query, cliccando due volte su ciascun campo si desideri aggiungere. In alternativa, è possibile aggiungere un campo alla query trascinandolo dalla tabella all'Area di visualizzazione.

- Creare una query in Visualizzazione SQL.
  1. In **Microsoft Query**, cliccare sul pulsante **SQL** e digitare la propria Istruzione SQL, per esempio:

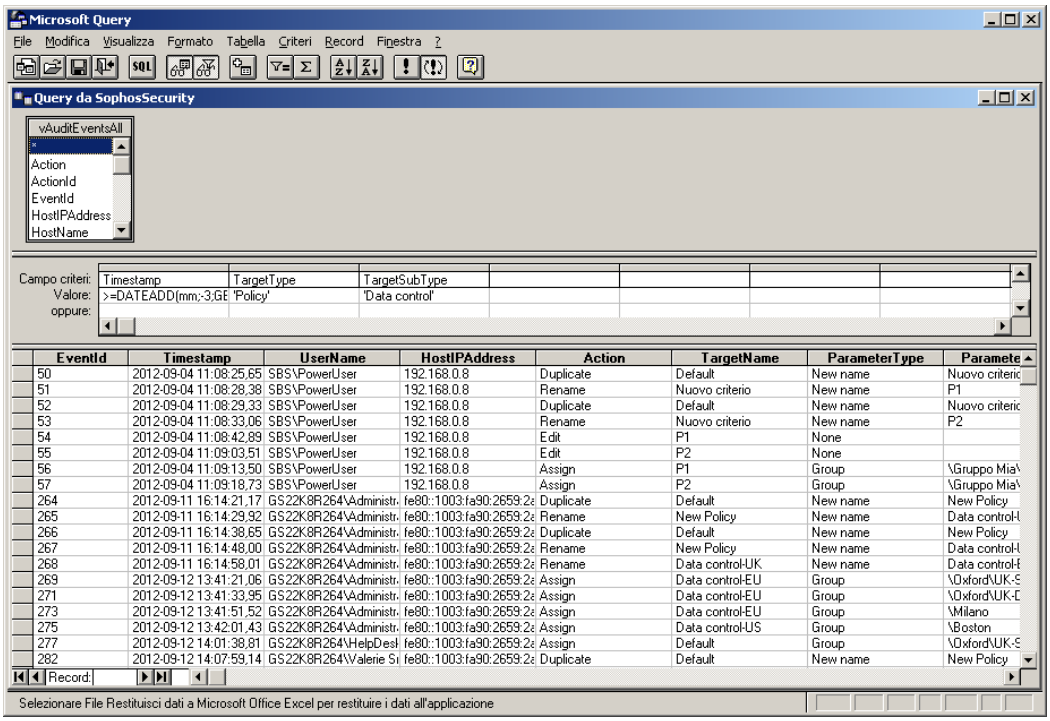
```
SELECT EventId, Timestamp, UserName, HostIPAddress, Action,
 TargetName, ParameterType, ParameterValue, Result

FROM SophosSecurity.Reports.vAuditEventsAll

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

ORDER BY EventId ASC
```

  Cliccare su **OK**.



4. Per salvare la query, dal menu **File**, cliccare su **Salva**.

7.3 Restituzione dei dati a Excel

1. Per tornare ad Excel, nella finestra di dialogo **Microsoft Query**, cliccare sul pulsante **Restituisci dati**.

   In alternativa, dal menu **File**, cliccare su **Restituisci dati a Microsoft Excel in Microsoft Query**.

   In Excel, viene visualizzata la finestra di dialogo **Importa dati**, in cui è possibile scegliere quale tipo di report creare.

   Il seguente esempio mostra la:

   - Creazione di una tabella a pagina 16
   - Creazione di un report Tabella pivot a pagina 17

7.4 Creazione di una tabella

1. Se si desidera importare i dati di controllo in una tabella Excel, nella finestra di dialogo **Importa dati**, lasciare selezionata l'opzione **Tabella**.

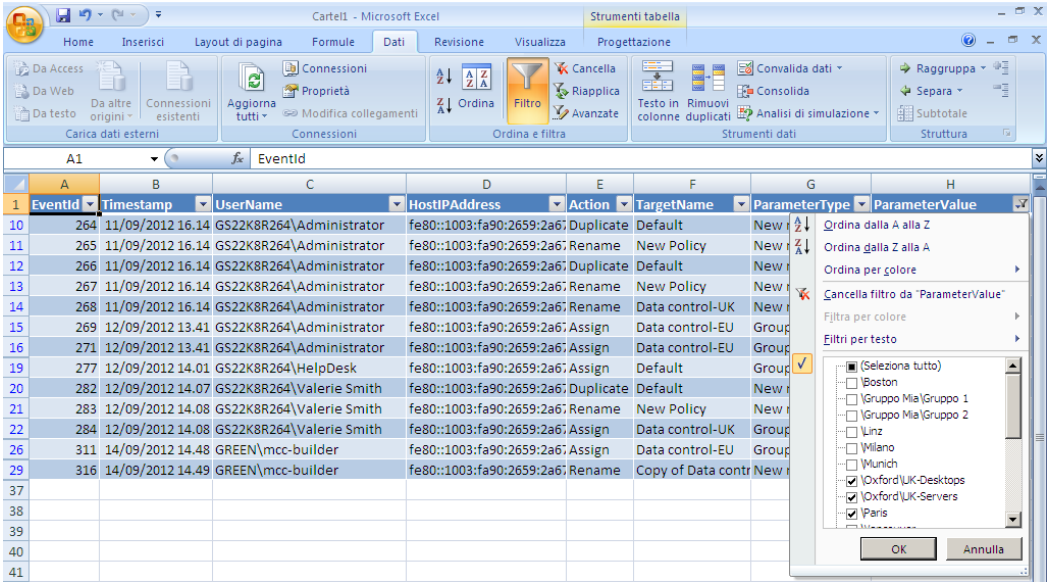
   Per inserire i dati nel foglio di lavoro esistente, a partire dalla cella A1, lasciare selezionata l'opzione **Foglio di lavoro esistente**:

   Cliccare su **OK**.

   I dati di controllo sono stati ora importati nella tabella Excel.

2. Salvare la propria Cartella di lavoro di Excel.

3. È possibile utilizzare "Filtro di ricerca" per analizzare i dati ora a disposizione.



7.5 Creazione report Tabella pivot

1. Se si desidera importare i dati di controllo in una tabella Excel, nella finestra di dialogo **Importa dati**, selezionare **Rapporto di tabella pivot**.

   Per inserire i dati nel foglio di lavoro esistente, a partire dalla cella A1, lasciare selezionata l'opzione **Foglio di lavoro esistente**:

   Cliccare su **OK**.

   La tabella vuota "tabella pivot" viene visualizzata nel foglio di lavoro.

2. In **Elenco campi tabella pivot**, visualizzato a destra, selezionare i campi che si desidera visualizzare.

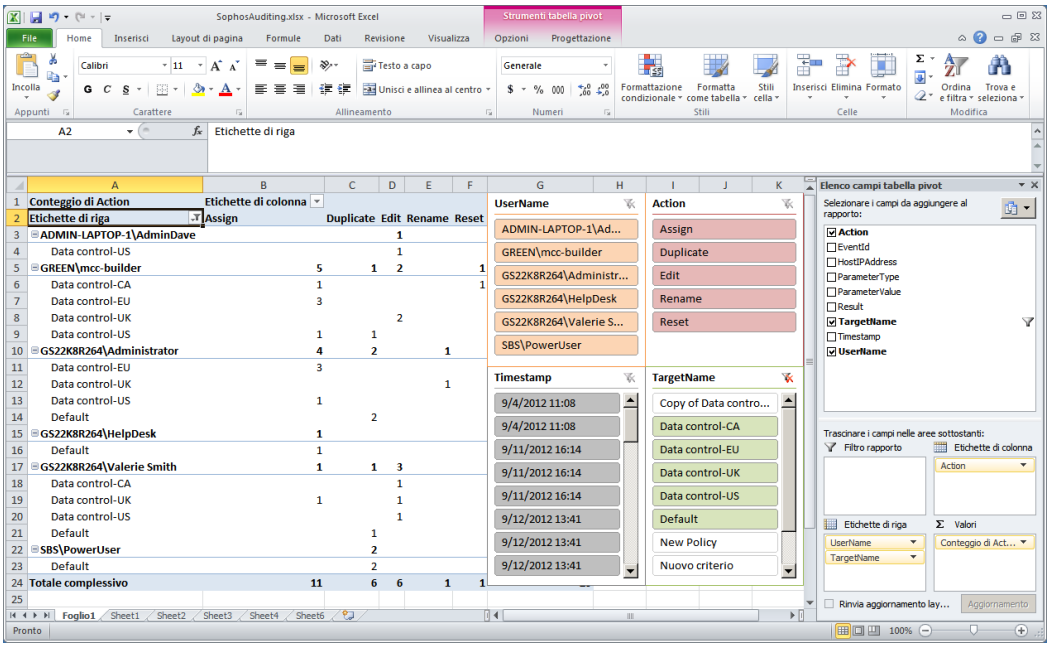
   Suggerimento: È possibile filtrare i dati prima di aggiungere i campi. In **Elenco campi tabella pivot**, nella casella **Selezionare i campi da aggiungere al rapporto**, posizionare il puntatore nel campo relativo al nome, quindi cliccare sulla freccia in giù del filtro di fianco al campo del nome. Dal menu **Filtro**, scegliere l'opzione di filtro desiderata.

3. A seconda di come si desidera visualizzare la "tabella pivot", trascinare i campi fra le aree dell'**Elenco campi tabella pivot**. Si potrebbe per esempio decidere di visualizzare i nomi degli utenti e i criteri da essi modificati come righe della tabella, mentre le azioni eseguite dagli utenti sui criteri potrebbero essere le etichette di colonna.

4. Per poter applicarli filtri alla tabella pivot, sotto **Strumenti tabella pivot**, andare a **Opzioni** e cliccare su **Inserisci filtro dati**.
5. Nella finestra di dialogo **Inserisci filtro dati**, selezionare il filtro dati che si desidera utilizzare e cliccare su **OK**.

   È possibile riorganizzare il filtro dati nel foglio di lavoro selezionando un filtro dati e rilasciandolo nella posizione desiderata. È inoltre possibile personalizzare il filtro dati, per esempio attribuendo colori diversi. Per far ciò, selezionare il filtro dati. Sotto **Strumenti filtro dati**, **Opzioni** e quindi selezionare **Stili del filtro strumenti**.

   La tabella pivot potrebbe assomigliare a questa:



6. Salvare la propria Cartella di lavoro.

8 Ulteriori esempi sulla creazione di un report di controllo

Questa sezione spiega come creare una query nuova da una fonte dei dati esistente in Microsoft Excel, oltre che fornire ulteriori esempi di query da utilizzare per creare report di controllo.

Questa sezione descrive inoltre come creare un report comprensivo di informazioni dettagliate sulle modifiche apportate ai criteri in formato XML.

8.1 Creazione di una query da una fonte dei dati esistente

Per generare un report di controllo aggiuntivo dalla fonte dei dati creata in Impostazione di una connessione al database a pagina 12:

1. In Excel, andare alla scheda **Dati**, cliccare su **Da altre origini**, e quindi su **Da Microsoft Query**.
2. Nella finestra di dialogo **Scegli origine dati**, deselezionare la casella di spunta **Usa Creazione guidata Query per creare/modificare query**. Selezionare la fonte dei dati creata in precedenza (per es. SophosAuditing) e cliccare su **OK**.
3. In **Microsoft Query**, cliccare sul pulsante **SQL** e inserire un'Istruzione SQL, per il report.

La seguente sezione riporta alcuni esempi che possono essere utilizzati.

8.2 Ulteriori esempi di query

Esempio 1: quali criteri sono stati modificati negli ultimi 60 giorni da un determinato utente

```
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
```

Nota: In un'istruzione SQL, invece che elencare i campi da includere nel report, digitare "SELECT *" per selezionare tutti i campi della vista database.

Esempio 2: quali criteri erano stati applicati a un determinato gruppo negli ultimi sei mesi

```
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
```

Nota: Se il gruppo per cui si sta creando un report è il sottogruppo di un altro gruppo, sarà necessario digitare il percorso completo del gruppo o utilizzare l'istruzione "termina con" (se il nome del gruppo è univoco). Per esempio, se si desidera creare un report per il gruppo \Oxford\UK-Servers, è possibile utilizzare una delle seguenti opzioni:

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

Esempio 3: quali modifiche sono state apportate al gruppo negli ultimi tre mesi da un determinato utente

La seguente istruzione porterà alla creazione di un report in cui verranno elencati i gruppi creati, cancellati, spostati o rinominati, oltre che i computer assegnati ai gruppi dall'utente negli ultimi tre mesi.

```
SELECT *

FROM SophosSecurity.Reports.vAuditEventsAll

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

Esempio 4: quali modifiche sono state apportate a determinati gruppi negli ultimi tre mesi

```
SELECT *

FROM SophosSecurity.Reports.vAuditEventsAll

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

8.3 Restituzione dei dati a Excel

Una volta creata una query per il report di controllo, riportare i dati in Excel (**File** > **Restituisci dati a Microsoft Excel in Microsoft Query**) e creare un report secondo quanto descritto nelle sezioni Creare una tabella a pagina 16 o Creazione report Tabella pivot a pagina 17.

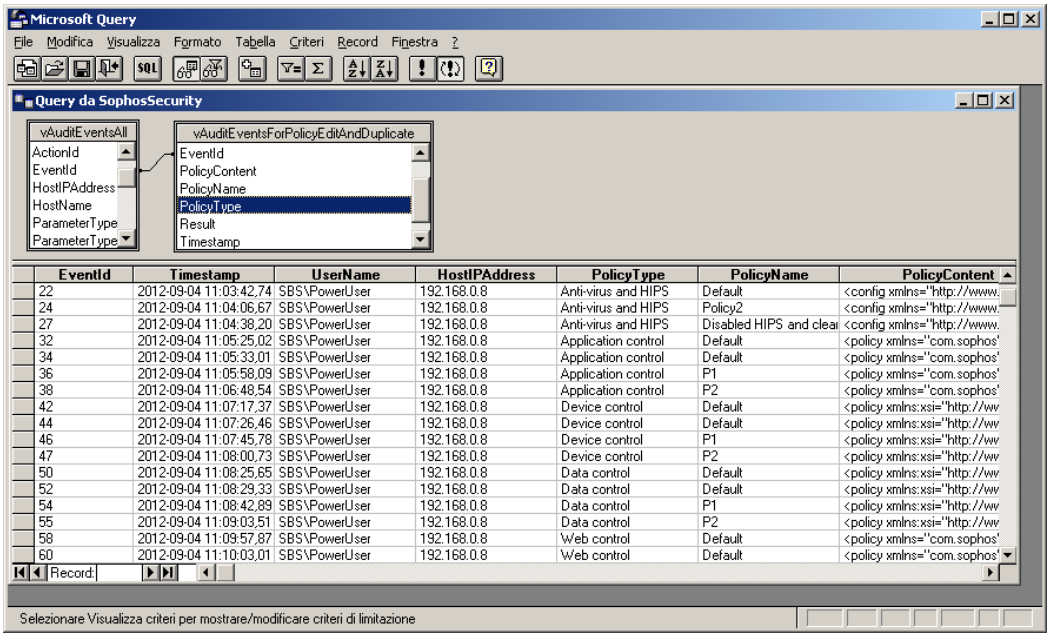
8.4 Creazione di un report contenente le modifiche ai criteri in formato XML

Quando un utente modifica un criterio, le impostazioni del criterio selezionate vengono salvate in formato XML e vi si può accedere tramite la vista del database **Reports.vAuditEventsForPolicyEditAndDuplicate**.

È possibile creare un report contenente questi dati aggiuntivi collegando le due tabelle, **Reports.vAuditEventsAll** e **Reports.vAuditEventsForPolicyEditAndDuplicate**.

1. Creare una nuova query da una fonte dei dati esistente, come descritto nella sezione Creazione di una query da una fonte dei dati esistente a pagina 19.
2. In **Microsoft Query**, cliccare su **Table** e quindi su **Add Tables**. Nella finestra di dialogo **Add Tables**, selezionare **vAuditEventsForPolicyEditAndDuplicate** e cliccare su **Add**. una volta portata a termine questa operazione, cliccare su **Close**.
3. Collegare le tabelle creando collegamenti fra i campi che le due tabelle hanno in comune. Cliccare sul campo comune, **EventID**, della prima tabella e trascinarlo sul campo **EventID** della seconda tabella.
4. Aggiungere campi alla query cliccandovi due volte. In alternativa, è possibile aggiungere un campo alla query trascinandolo dalla tabella all'Area di visualizzazione.

   Suggerimento: È possibile utilizzare la finestra di dialogo **Joins** in Microsoft Query (**Table** > **Joins**) per creare una query fondendo due tabelle.



5. Per salvare la query, dal menu **File**, cliccare su **Salva**.

6. Per tornare a Excel, cliccare sul pulsante **Restituisci dati**.

In alternativa, dal menu **File**, cliccare su **Restituisci dati a Microsoft Excel in Microsoft Query**.

In Excel, si apre la finestra di dialogo **Importa dati**. Creare una tabella (Creazione di una tabella a pagina 16). La colonna **PolicyContent** includerà le modifiche apportate alla configurazione del criterio in formato XML.

Suggerimento: Se si esegue Microsoft SQL Server Management Studio, è possibile richiamare la query direttamente dalla vista **Reports.vAuditEventsForPolicyEditAndDuplicate**. Quando si clicca sul collegamento nella colonna **PolicyContent** relativa ai risultati della query, il contenuto del criterio verrà visualizzato in un editor XML in un formato più facilmente leggibile all'interno di una tabella Excel.

9 Azioni sottoposte a controllo

Le categorie di azioni sottoposte a controllo includono:

- Azioni del computer
- Gestione di gruppi di computer
- Gestione criteri
- Gestione dei ruoli
- Gestione di Sophos Update Manager
- Eventi di sistema

9.1 Azioni del computer

Le seguenti azioni del computer vengono sottoposte a controllo:

- Cancellazione/risoluzione di allarmi ed errori
- Protezione di un computer
- Aggiornamento di un computer
- Cancellazione di un computer
- Esecuzione della scansione completa del sistema del computer

9.2 Gestione di gruppi di computer

Le azioni registrate per la gestione dei gruppi sono:

- Creazione di un gruppo
- Cancellazione di un gruppo
- Spostamento di un gruppo
- Rinomina di un gruppo
- Assegnazione di un computer a un gruppo

9.3 Gestione criteri

Le azioni registrate per la gestione dei criteri sono:

- Creazione di un criterio a pagina 24
- Rinomina di un criterio
- Duplicazione di un criterio a pagina 24
- Modifica un criterio
- Assegnazione di un criterio a un computer
- Ripristino di un criterio alle impostazioni predefinite

- Cancellazione di un criterio a pagina 24

9.3.1 Creazione di un criterio

Quando si crea un nuovo criterio, il criterio predefinito viene duplicato e la sua copia, denominata "Nuovo criterio", funziona da base per il nuovo criterio. È possibile cambiare il nome del nuovo criterio nonappena creato. Per esempio, se si crea un criterio Anti-Virus e HIPS e lo si rinomina con la dicitura "Server", verranno create le seguenti voci di controllo:

Tabella 1: Creazione di un nuovo criterio e attribuzione di un nuovo nome

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	Server	Success

9.3.2 Duplicazione di un criterio

Quando si duplica un criterio, viene creato un evento di "Duplicazione di un criterio", per esempio:

Tabella 2: Duplicazione di un criterio

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 Cancellazione di un criterio

Quando si cancella un criterio, qualsiasi gruppo che utilizza il criterio cancellato tornerà a utilizzare quello predefinito. In questo caso, non viene creato alcun evento di controllo separato indicante che è stato riapplicato il criterio predefinito.

9.4 Gestione dei ruoli

Le azioni registrate per la gestione dei ruoli sono:

- Creazione di un ruolo
- Cancellazione di un ruolo
- Rinomina di un ruolo

- Duplicazione di un ruolo
- Aggiunta di un utente a un ruolo
- Rimozione di un utente da un ruolo
- Aggiunta di un diritto a un ruolo
- Rimozione di un diritto da un ruolo

9.5 Gestione di Sophos Update Manager

Le azioni registrate per la gestione di Sophos Update Manager sono:

- Aggiornamento del gestore aggiornamenti
- Allineamento del gestore aggiornamenti alla configurazione
- Cancellazione allarmi
- Cancellazione del gestore aggiornamenti
- Configurazione del gestore aggiornamenti

9.5.1 Modalità di registrazione delle modifiche apportate alla configurazione di Update Manager

In Enterprise Console, la finestra di dialogo **Configura il gestore aggiornamenti** include una serie di schede e opzioni che rappresentano essenzialmente i criteri di configurazione del gestore degli aggiornamenti. Quando si apportano modifiche alla configurazione del gestore degli aggiornamenti, vengono registrate le seguenti azioni nei criteri:

- **Update Manager - subscription** - specifica le sottoscrizioni software che il gestore aggiornamenti continua ad aggiornare.
- **Update Manager - upstream** - specifica la fonte degli aggiornamenti per il gestore aggiornamenti.
- **Update Manager - downstream** - specifica le condivisioni in cui il gestore aggiornamenti scarica il software.
- **Update Manager - schedule** - specifica la frequenza con cui il gestore aggiornamenti verifica la presenza di dati sul rilevamento delle minacce di aggiornamenti software.
- **Update Manager - general** - specifica le opzioni di accesso per il gestore aggiornamenti.
- **Software subscription** - specifica la configurazione delle sottoscrizioni software, per es. "Consigliata".

A volte le modifiche apportate a un criterio del gestore aggiornamenti possono innescare ulteriori cambiamenti in altri criteri del gestore aggiornamenti (per es. quando viene cambiato il valore ID). In questi casi verranno registrati molteplici record nel database SophosSecurity, sebbene la modifica apportata sia una. Per esempio, se si crea una pianificazione nella scheda **Operazione pianificata** della finestra di dialogo **Configura il gestore aggiornamenti** e cliccare su OK, verranno create le seguenti voci di controllo:

Tabella 3: Creazione di una pianificazione aggiornamenti per 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 questo caso, solo la prima azione, registrata nel criterio **Update Manager - schedule**, rispecchia un'effettiva modifica alla configurazione. Tutte le altre modifiche al criterio registrate per questo evento sono solo cambiamenti del parametro ID interno. Per verificare quali modifiche siano state apportate, è possibile utilizzare la vista **Reports.vAuditEventsForPolicyEditAndDuplicate** del database SophosSecurity, secondo quanto descritto nella sezione Creazione di un report contenente le modifiche ai criteri in formato XML a pagina 21.

9.6 Eventi di sistema

I seguenti eventi di sistema sono sottoposti a controllo:

- Abilitare la funzione di controllo.
- Disabilitare la funzione di controllo.

10 Campi dati di Sophos Auditing

Le seguenti viste del database, o fonti dei dati, sono disponibili per Sophos Auditing:

- Reports.vAuditEventsAll
- Reports.vAuditEventsForPolicyEditAndDuplicate

I campi dati disponibili per ciascuna di queste fonti dei dati sono elencati di seguito. Tutte le colonne della data e ora esprimono valori in Tempo universale coordinato (UTC), nel formato "anno-mese-giorno hh:min:ss" (24 ore). I campi comuni a entrambi gli elenchi sono messi in evidenza in grassetto.

Reports.vAuditEventsAll

La vista del database **Reports.vAuditEventsAll** include l'elenco completo degli eventi di controllo, oltre che la molte informazioni relative alla funzione di controllo.

Campo dati	Tipo di dati	Descrizione
EventId	integer	Un ID numerico univoco dell'evento.
Timestamp	datetime	La data e l'ora in cui si è verificata l'azione registrata nell'evento.
Action	nvarchar(128)	L'azione registrata nell'evento, per es. Crea, Modifica, Rinomina, Assegna, Cancella.
TargetType	nvarchar(128)	Il tipo di oggetto o l'impostazione di configurazione modificato dall'azione, per es. Groppo, Computer, Criterio, Ruolo.
TargetSubType	nvarchar(128)	Il sotto-tipo dell'oggetto o l'impostazione modificato dall'azione, quando applicabile. Per es. il nome del criterio modificato, quali Anti-virus e HIPS o Data control.
TargetName	nvarchar(4000)	Il nome dell'oggetto o dell'impostazione modificata dall'azione, per es. il nome definito dall'utente del criterio o del gruppo.
ParameterType	nvarchar(128)	Il tipo della nuova impostazione od oggetto assegnato alla destinazione. Per es. per Action="Rename" e TargetType="Policy", ParameterType="New name". Per Action="Assign" e TargetType="Computer", ParameterType="Group".

Campo dati	Tipo di dati	Descrizione
ParameterValue	nvarchar(4000)	Il valore della nuova impostazione od oggetto, per es. il nuovo nome definito dall'utente del criterio o il nuovo gruppo a cui è stato assegnato il computer.
Result	nvarchar(128)	Il risultato dell'azione, avente il valore "Positivo" o "Negativo".
UserName	nvarchar(256)	Il nome dell'utente che ha eseguito l'azione.
HostName	nvarchar(256)	Il nome del computer da cui l'utente ha eseguito l'azione.
HostIPAddress	nvarchar(48)	L'indirizzo IP del computer da cui l'utente ha eseguito l'azione. Se le connessioni di rete fra server e Enterprise Console avvengono tramite IPv6, gli indirizzi IPv6 verranno registrati. In caso contrario, verranno registrati gli indirizzi IPv4.
ActionId	integer	Un ID numerico univoco dell'azione.
TargetTypeId	integer	Un ID numerico univoco del tipo di destinazione.
TargetSubTypeId	integer	Un ID numerico univoco del sotto-tipo di destinazione.
ParameterTypeId	integer	Un ID numerico univoco del tipo di parametro.
SubEstateId	integer	Un ID numerico univoco del sottoambiente dell'utente.
ResultId	integer	Un ID numerico univoco del risultato, 1 (positivo) o 0 (negativo).
UserSid	nvarchar(128)	L'identificatore di sicurezza dell'utente.

Reports.vAuditEventsForPolicyEditAndDuplicate

La vista del database **Reports.vAuditEventsForPolicyEditAndDuplicate** include informazioni relative alle modifiche apportate al criterio.

Campo dati	Tipo di dati	Descrizione
EventId	integer	Un ID numerico univoco dell'evento.

Campo dati	Tipo di dati	Descrizione
Timestamp	datetime	La data e l'ora in cui si è verificata l'azione registrata nell'evento.
Action	nvarchar(128)	L'azione registrata nell'evento.
Result	nvarchar(128)	Il risultato dell'azione, avente il valore "Positivo" o "Negativo".
PolicyType	nvarchar(128)	Il tipo di criterio modificato dall'azione, per es. Anti-virus and HIPS o Web Control.
PolicyName	nvarchar(4000)	Il nome definito dall'utente del criterio.
PolicyContent	XML	Le modifiche apportate al frammento della configurazione del criterio, in formato XML.
UserName	nvarchar(256)	Il nome dell'utente che ha eseguito l'azione.

11 Risoluzione dei problemi

Quando Sophos Auditing non riesce, viene registrato un evento nel registro eventi applicazioni di Windows avente come fonte "Sophos Auditing". Ciò avviene di solito quando si verifica un problema di connettività del database.

12 Appendice: ID numerici dei valori del campo dati

Le seguenti tabelle mostrano ID numeriche uniche relative ad alcuni valori dei campi dati di Sophos Auditing.

Si consiglia l'utilizzo queste ID numeriche piuttosto che valori stringa, se si desidera attribuire un ordine logico ai dati di controllo esportati. Ciò può evitare problemi di compatibilità nel caso valori stringa vengano modificati nei rilasci futuri di Enterprise Console.

Campo dati	Valore campo dati	ID numerica
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

Campo dati	Valore campo dati	ID numerica
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
	Tamper protection	19

Campo dati	Valore campo dati	ID numerica
	Web control	22
	Prevenzione degli exploit	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 Supporto tecnico

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

- Visitare la Sophos Community su community.sophos.com/ e cercare altri utenti che hanno riscontrato lo stesso problema.
- Visitare 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.

14 Note legali