SOPHOS

Cybersecurity made simple.

Sophos Enterprise Console 审核指南

产品版本号： 5.5

内容

1 关于本指南

本指南向您介绍如何监控 Sophos Enterprise Console 配置的变化以及其他用户和系统操作。

2 关于 Sophos Auditing

Sophos Auditing 使您能够监控 Enterprise Console 的配置所发生的更改，以及其它用户和系统的操作行为。您可以在规范遵照和排疑解难时使用此（审核）信息，或者，在发生恶意入侵活动时，使用此信息进行证据采集与分析。

依照默认值，审核是禁用的。在 Enterprise Console 中启用了审核功能后，每当某些配置设置被更改时，或者，某些操作被执行时，都会有审核记录被写入 SQL Server 数据库中。

审核记录包括以下信息：

- 执行的操作
- 执行操作的用户
- 用户的计算机
- 用户的子领域
- 操作的日期和时间

无论是成功的操作，还是失败的操作，两者都会被审核，因此，审核记录会显示谁在系统中之行了操作，谁进行了最终没有成功的操作。

您可以使用第三方的软件，如：Microsoft Excel，Microsoft Access，Microsoft SQL Server Reporting Services，或者 Crystal Reports 等，访问和分析存储在审核数据库中的数据。

重要提示
通过 Sophos Auditing 可以向第三方的应用程序提供数据。使用这一功能时，您要确保已落实了负责数据安全的责任，并且只有经授权的用户才能访问它们。有关安全注意事项，请参阅内建数据库保护 （第 4 页）。

要了解更多有关哪些操作会被审核的信息，请参阅会审核哪些操作 （第 19 页）。

3 使用 Sophos Auditing 的关键步骤

使用 Sophos Auditing 的关键步骤有：

- 确保数据库是安全的
- 启用审核
- 授权访问审核数据
- 创建审核报告

4 确保数据库是安全的

4.1 内建数据库保护

Enterprise Console 和 SophosSecurity 数据库为审核数据提供了数种内建的保护类型：

- 访问控制
- 介入防范

访问控制

访问控制在以下级别中实施：

- 前端图形用户界面 (GUI) 级别

  只有在 Enterprise Console 中具备 审核 权限，并且是 Sophos Console Administrators 组成员的用户，才能启用或禁用审核。

- 数据库级别

  依照默认值，只有 Sophos DB Admins 组成员的用户才能访问数据库界面。另外，来自数据库界面的存储过程要求提供有效的用户会话令牌。当用户开启 GUI 或更改子领域时，系统会生成该令牌。

介入防范

数据库已被设计为可以防止更改审核事件的数据。除了某些配置设置之外，您不需要更新审核数据库中的任何数据。设定了某些触发条件，它们会回滚任何试图从数据库表中更新或删除数据的操作。

这些数据只能在清空数据库时才会被删除。保存了两年以上的数据会被自动清除，清除工作会每 24 小时进行一次，它是在 Enterprise Console 服务器上内置的标准计划清空任务的一部分。您还可以使用 PurgeDB 工具清空数据（请参阅 http://www.sophos.com/en-us/support/knowledgebase/109884.aspx）。

4.2 加强数据安全

审核数据库

除了在 数据库内置保护措施外，我们还建议在 SQL Server 实例设置附加的保护，以审核用户活动和对 SQL Server 做的更改。

例如，如果您使用企业版的 SQL Server 2008，您可以使用 SQL Server Audit 功能。较早版本的 SQL Server 支持使用内建的追踪机制，进行登录审核，基于触发条件的审核，和事件审核。

要了解有关您可以用来审核在 SQL Server 系统中发生的活动和更改的审核功能的更多信息，请参见您所使用的 SQL Server 版本的技术文档。例如：

- SQL Server Audit (Database Engine)（英文）
- Auditing (Database Engine), SQL Server 2008 R2

- Auditing in SQL Server 2008
- Auditing (Database Engine), SQL Server 2008

加密到数据库的连接

我们强烈建议您加密任何客户端与 数据库之间的连接。要了解更多信息，请参见 SQL Server 技术文档：

- Enable Encrypted Connections to the Database Engine (SQL Server Configuration Manager)（英文）
- Encrypting Connections to SQL Server 2008 R2（英文）
- How to enable SSL encryption for an instance of SQL Server by using Microsoft Management Console（英文）

控制对数据库备份的访问权限

请确保对有何数据库备份或复制文件有适当的，限制性的访问权限控制。这将确保未经授权的用户无法访问文件，篡改文件，或者，无意中删除文件。

注释
使用本节中的链接可方便您查看第三方提供的信息。我们会定期对链接的精确度进行检查，但这些链接也可能会在我们不知情的情况下发生更改。

数据库连接检查

运行 5.5.1 安装程序时，将进行数据库连接检查（在安装或升级前），以确定是否可以使用 TLS 1.2 连接到数据库。

为确保在连接到数据库时使用 TLS 1.2，请使用 CheckDBConnection.exe 工具提供有关连接检查的输出并进行手动修改。

有关详细信息，请参阅知识库文章 127521。

5 启用 Sophos Auditing

依照默认值，审核功能是禁用的。要启用审核功能：

1. 在 Enterprise Console 的 工具 菜单中，单击 管理审核。
2. 在 管理审核 对话框中，勾选 启用审核 勾选框。

> 注释
> 如果该选项是灰白显示的，那么，说明您没有管理审核的权限。您必须是 Sophos Console Administrators 组的成员，并且在 Enterprise Console 中具备 审核 权限，以便能够启用或禁用审核。要了解更多有关用户权限和基于角色的管理的信息，请参见 Sophos Enterprise Console 帮助。

6 授权访问审核数据

依照默认值，只有系统管理员可以访问审核数据。其他需要访问数据创建审核报告的用户，需要明确地被授与 SophosSecurity 数据库的 Reports 架构的“选择”权限。这可以通过使用 sqlcmd 实用工具来做到，或在 SQL Server Management Studio 中来完成。

6.1 使用 sqlcmd 实用工具授权访问审核数据

要授权访问审核数据：

1. 将以下脚本复制并保存为纯文本文件，例如：记事本文件。

```
USE SophosSecurity;

DECLARE @stmt NVARCHAR(max);

DECLARE @Account VARCHAR(512)

/* 用被授权访问审核数据的实际帐户，替换 <域>\<用户>。*/

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. 请将 "SET @Account = N'<Domain>\<User>'" 中的 <Domain> and <User> 替换为您想要授权访问的用户的域和用户名。

   如果您的计算机是在工作组中，请将 <Domain> 替换为安装了数据库的那台计算机的名称。如果用户会从不同的工作组计算机上访问数据，那么，用户帐户必须在这些计算机上存在，并且使用相同的用户名和密码。

3. 打开命令行提示窗。
4. 连接到 SQL Server 实例 (instance)。键入：

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

   默认的 SQL Server 实例 (instance) 是 SOPHOS。

5. 将脚本从先前保存的纯文本文件中复制到命令行提示窗中。
6. 按 Enter 键，运行脚本。
   在脚本运行之后，用户会被授与 SophosSecurity 数据库的 报告 架构的 “选择” 权限，并且可以访问审核数据。
7. 请对每个需要访问权限的用户重复此步骤。

6.2 使用 SQL Server Management Studio 授权访问审核数据

在您能够授与 SQL Server Management Studio 中的用户，SophosSecurity 数据库的 Reports 架构的“选择”权限之前，请确保该用户可以登录 SQL Server，并且是 SophosSecurity 数据库的用户。

- 如果该用户已经可以登录 SQL Server，请将它添加为 SophosSecurity 数据库用户。在对象资源管理器中，展开服务器，展开 数据库 文件夹，展开 SophosSecurity，然后，展开 Security。右击 用户，然后，单击 新建用户。在 数据库用户 对话框中，输入用户名，并选择登录名。单击 确定。

  要了解更多有关创建数据库用户的信息，请参阅http://msdn.microsoft.com/en-us/library/aa337545.aspx#SSMSProcedure。

- 如果用户不能登录 SQL Server，请添加新的 SQL Server 登录名，并使它成为 SophosSecurity 数据库用户。在对象资源管理器中，展开服务器，展开 Security。右击 登录名，然后，单击 新建登录。在 登录 对话框中的 常规 页面，输入帐户名或组名。转到 用户映射 页中，并选择 SophosSecurity。单击 确定。

  要了解更多有关创建 SQL Server 登录名的信息，请参阅http://msdn.microsoft.com/en-us/library/aa337562.aspx#SSMSProcedure。

要在 SQL Server Management Studio 中授权用户访问审核数据：

1. 在对象资源管理器中，展开服务器，展开 数据库 文件夹，展开 SophosSecurity，展开 Security，然后展开 Schemas。
2. 右击 Reports，然后单击 Properties。
3. 在 Schema Properties - Reports 对话框中的 Permissions 页面中，单击 Search。在 Select Users or Roles 对话框中，添加一个或多个用户。
4. 每个用户都应该在 〈用户〉 “权限”中的 显式 选项卡，选取 授权下的 选择，接着单击 确定。

7 在 Microsoft Excel 中创建审核报告

此示例将向您显示怎样从 SQL Server 数据库中导入审核数据，并在 Microsoft Excel 2010 中分析这些数据。

以下将说明怎样通过几个关键步骤在 Microsoft Excel 中创建审核报告：

- 建立到审核数据库的连接（创建新的数据源）。
- 在 Microsoft Query 中创建查询。
- 返回数据到 Excel。
- 在 Excel 中创建报告（表或数据透视表的报告）。

注释
如果您想要绑定任何外部逻辑到导出的审核数据上，我们建议使用数字 ID，而不使用字符串值。例如，不使用 TargetType 字段的值，而是使用 TargetTypeId 字段的值。这有助于避免将来发布 Enterprise Console 时，由于任何字符串的更改，而可能产生的兼容性问题。要了解数字 ID 表，请参阅附录：数据字段值的数字 ID （第 26 页）：

要了解更多有关导入 SQL Server 数据和在 Excel 中创建报告的信息，请参见 Microsoft 的技术文档。

7.1 建立到数据库的连接

首先，您需要建立到数据库的连接。

1. 打开 Excel。在 数据 标签页的 获取外部数据 组中，单击 从其它数据源，然后，单击 从 Microsoft Query。
   会出现 选择数据源 对话框。
2. 在 数据库 标签中，保留勾选 <新建数据库源>，然后单击“确定”。
3. 在 创建新的数据源 对话框中，输入您的数据源的名称。在此例中，我们命名它为 SophosAuditing。
4. 在 为您想要访问的数据库选择驱动程序 文本框中，选择 SQL Server。

单击 连接。

5. 在 SQL Server 登录 对话框的 服务器 文本框中，输入您想要连接的 SQL Server 服务器的名称。在此示例中，我们连接在同一台计算机（本地主机）上的 SOPHOS 数据库实例 (instance)。
6. 单击 选项 展开 选项 面板。在 数据库 对话框中，选择 SophosSecurity。

单击 确定。

7. 在 创建新数据源 对话框的 为您的数据源选择默认表（可选） 中，选择 vAuditEventsAll。单击 确定。

7.2 创建查询

此示例怎样对您刚创建的，有关过去 3 个月里数据控制策略的更改信息的数据源，进行查询。

1. 在 Choose Data Source 对话框中，取消勾选 Use the Query Wizard to create/edit queries 勾选框。
2. 选择您在先前步骤中创建的数据源（在此例中是 SophosAuditing），然后单击 确定。Microsoft Query 对话框中会显示 Query from SophosAuditing，并带有默认的表 vAuditEventsAll，它是您创建数据源时所选择的。
3. 执行下列操作之一：
   - 在设计视图中创建查询。
     a）在 Microsoft Query 对话框的 条件 菜单中，单击 添加条件。
     b）在 添加条件 对话框中的 字段 旁，选择 Timestamp。请确保 运算符 字段是空白的。在 值 字段中，键入：

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

     请使用在控制面板 区域和语言选项 设置，格式，附加的设置 中指定的列表分隔符。例如，如果您的列表分隔符是分号，那么，请在上面的语句中使用分号，而不是使用逗号。如果您使用了不正确的列表分隔符，您可能会收到出错消息 "Extra ')'"。

     单击 添加。该条件会被添加到 Query from SophosAuditing。
     c）在 添加条件 对话框中的 字段 旁，选择 TargetType。在 运算符 字段中，选择 等于。在 值 字段中，选择或键入 策略。

     单击 添加。该条件会被添加到 Query from SophosAuditing。
     d）在 添加条件 对话框中的 字段 旁，选择 TargetSubType。在 运算符 字段中，选择 等于。在 值 字段中，选择或键入 数据控制。

     单击 添加。该条件会被添加到 Query from SophosAuditing。

     在 添加条件 对话框中，单击 关闭。
     e）在 Microsoft Query 对话框中，从 vAuditEventsAll 中双击字段名，将字段添加到查询中。或者，您可以从表的显示区拖曳字段，将它添加到查询中。
   - 在 SQL 视图中创建查询。
     a）在 Microsoft Query，单击 SQL 按钮，然后输入您的报告的 SQL 语句，例如：

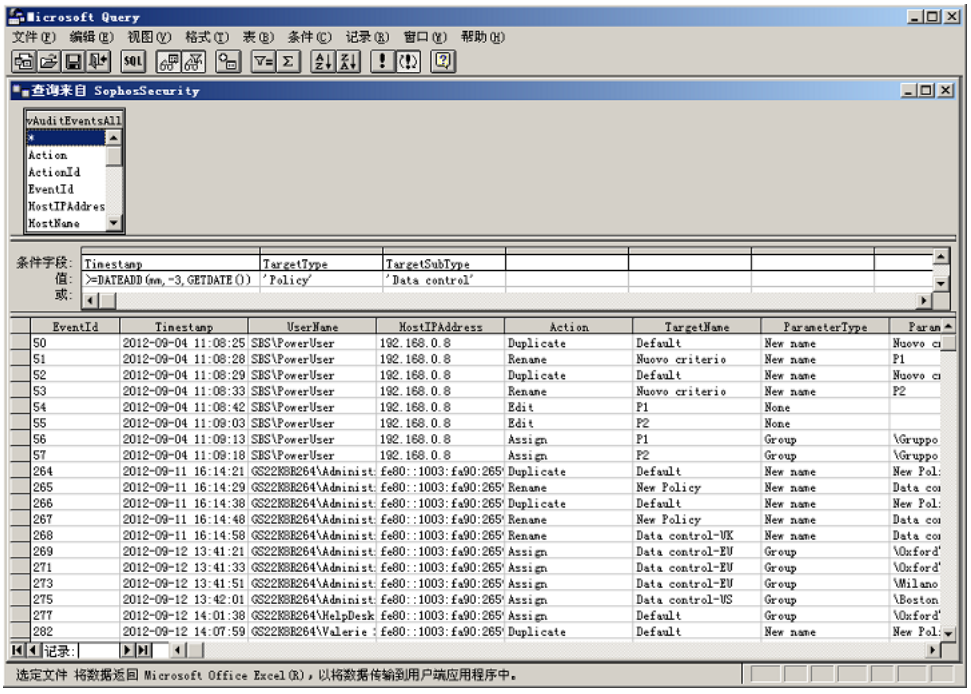
```
SELECT EventId, Timestamp, UserName, HostIPAddress, Action, TargetName,
 ParameterType, ParameterValue, Result

FROM SophosSecurity.Reports.vAuditEventsAll

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

ORDER BY EventId ASC
```

     单击确定。



4. 要保存查询，请在 文件 菜单中，单击 保存。

7.3 返回数据到 Excel

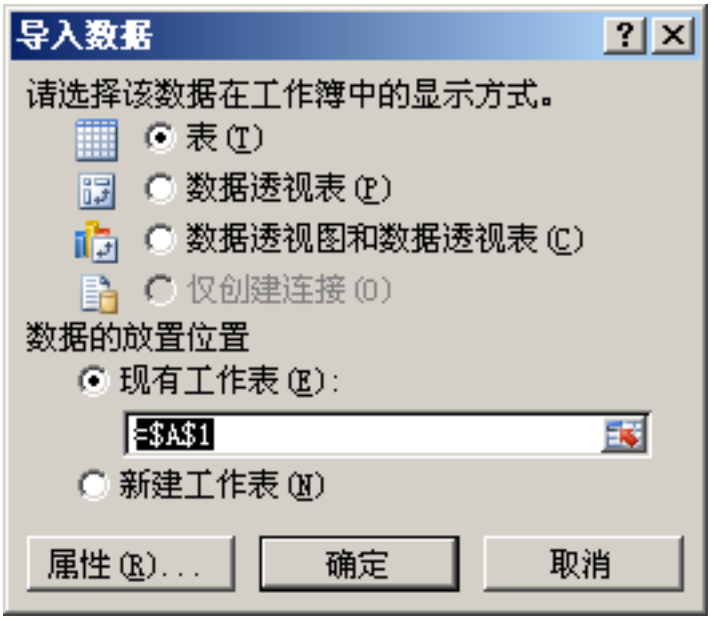
要返回到 Excel，请在 Microsoft Query 对话框中，单击 返回数据 按钮。

或者，在 文件 菜单中，单击 将数据返回到 Excel。
返回到 Excel 中，导入数据 对话框会出现，您可以在此对话框中，选择想要创建的报告的类型。
以下示例将说明怎样：

- 创建表 （第 12 页）
- 创建数据透视表报告 （第 13 页）

7.4 创建表

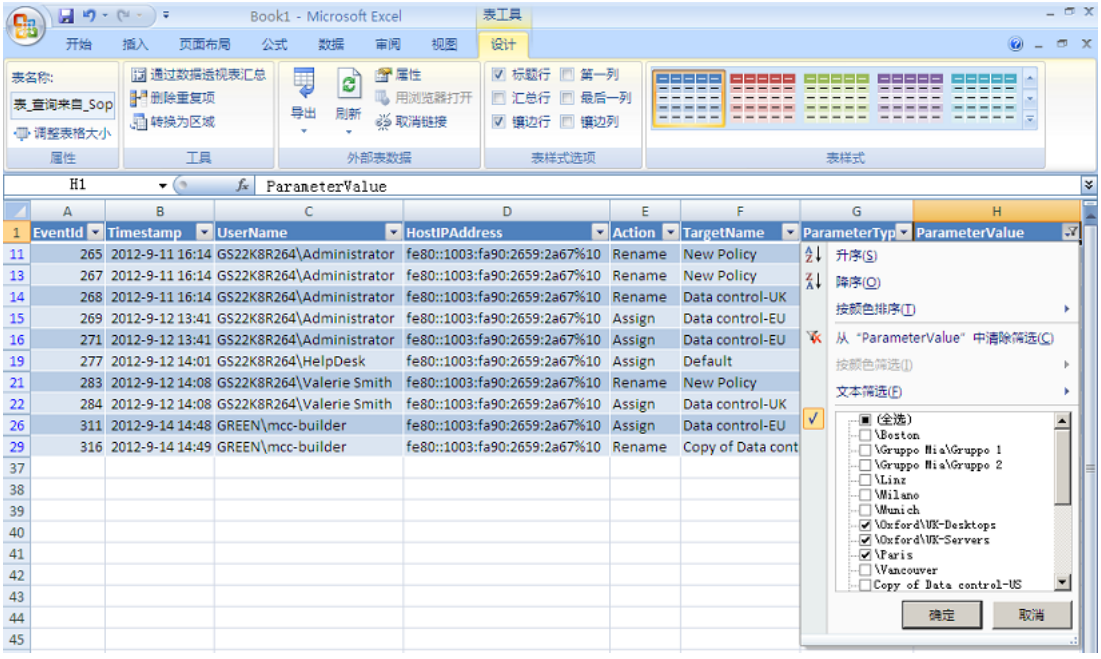
1. 如果您选择导入审核数据到 Excel 表中，那么，请在 导入数据 对话框中，保留勾选 表。
要将数据放入现有的工作表中，并从单元格 A1 开始，那么，请保留勾选 现有的工作表：



单击 确定。

审核数据会被导入 Excel 表中。

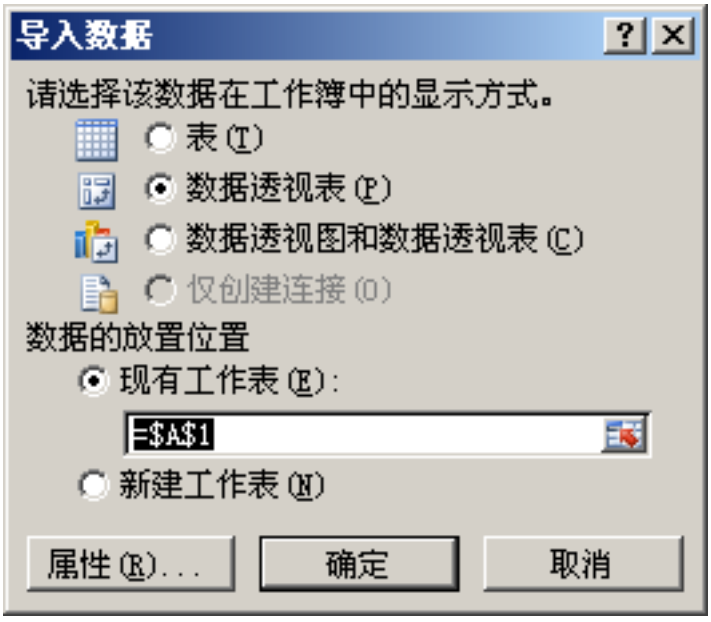
2. 保存您的 Excel 工作簿。
3. 您可以使用搜索过滤标准分析数据。



7.5 创建数据透视表报告

1. 如果您选择导入审核数据到 Excel 表中，那么，请在 导入数据 对话框中，保留勾选 数据透视表报告。

   要将数据放入现有的工作表中，并从单元格 A1 开始，那么，请保留勾选 现有的工作表：



单击 确定。

空白的数据透视表会出现在工作表中。

2. 在右边出现的 数据透视表字段列表 中，选择您想要查看的字段。

   提示
   您可以在添加字段之前，筛选数据。在 数据透视表字段列表 的 选择要添加到报表的字段 文本框中，请将指针停留在字段名上，然后单击字段名旁边的筛选器的下拉箭头。在 筛选器 菜单中，选择您想要的筛选器选项。

3. 根据您想要显示数据透视表的方式，在 数据透视表字段列表 的各个领域之间拖曳字段。例如，您可能想把用户名和与之相联系的策略显示为行标签，并将用户在策略中执行的操作显示为列标签。
4. 为了能够筛选数据透视表，请在 数据透视表工具 下的 选项 中，单击 插入切片器。
5. 在 插入切片器 对话框中，选择您想要使用的切片器，并单击 确定。

   通过选择切片器，并将它拖放到想要的位置，您可以在工作表中重新安排各个切片器。您还可以自定义切片器，比如，给它们加上不同的颜色。要这样做，请选择切片器。在 切片器工具 下的 选项 中，选择 切片器样式。
6. 保存您的工作簿。

8 创建审核报告的更多示例

本节将说明怎样从 Microsoft Excel 中现有的数据源创建新的查询，并且向您提供更多的查询示例，您可以用它们来创建审核报告。

本节还将说明怎样创建 XML 格式的，包含详细的策略更改信息的报告。

8.1 从现有的数据源创建查询

要从您在建立到数据库的连接 （第 9 页）中创建的数据源中创建另一个审核报告：

1. 在 Excel 中的 Data 标签页中，单击 From Other Sources，然后，单击 From Microsoft Query。
2. 在 Choose Data Source 对话框中，取消勾选 Use the Query Wizard to create/edit queries 勾选框。选择您先前创建的数据源（例如，SophosAuditing），然后，单击 OK。
3. 在 Microsoft Query，单击 SQL 按钮，然后输入您的报告的 SQL 语句。

以下部分包括您可以使用的一些示例。

8.2 查询的更多示例

示例 1：在过去的 60 天里，某人更改的那些策略。

```
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
```

注释
在语句中，您可以键入 "SELECT *" 以选择数据库视图中所有的字段，而不是列出您想要包括在报告中的字段。

示例 2：在过去的 6 个月里，应用到某个组的那些策略。

```
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
```

注释
如果您为其创建报告的组，是另一个组的子组，那么，您需要输入该组所在的完整路径，或者，使用 "ends with" 语句（前提是该组的组名是唯一的）。例如，要为组 \Oxford\UK-Servers 创建报告，您可以输入以下两者之一：

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

示例 3：在过去的 3 个月里，某人对某个组所做的那些更改。

以下语句将生成一个报告，显示创建，删除，移动，或重命名了哪些组，以及在过去 3 个月里，用户指派了哪些计算机到这些组。

```
SELECT *

FROM SophosSecurity.Reports.vAuditEventsAll

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

示例 4：在过去的 3 个月里，某个组发生的那些更改。

```
SELECT *

FROM SophosSecurity.Reports.vAuditEventsAll

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

8.3 返回数据到 Excel

在创建了针对审核报告的查询后，返回数据到 Excel（File > Return Data to Microsoft Excel），然后按照 创建表 （第 12 页） 或 创建数据透视表报告 （第 13 页） 中的说明，创建报告。

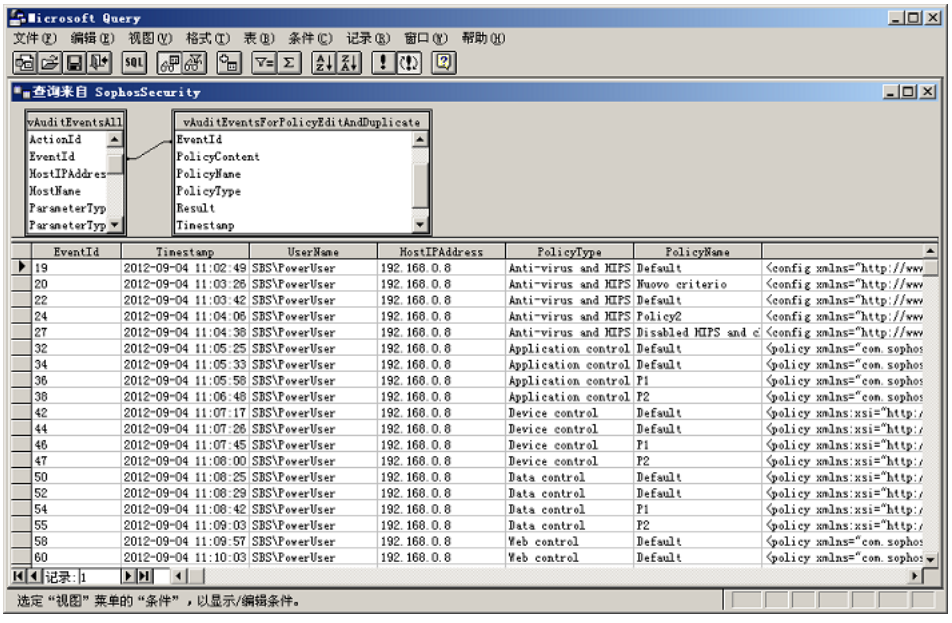
8.4 创建 XML 格式的策略更改报告

当用户编辑策略时，编辑之后的策略设置是以 XML 格式保存的，并且可以通过 Reports.vAuditEventsForPolicyEditAndDuplicate 数据库视图访问。

您可以通过连接到 Reports.vAuditEventsAll 和 Reports.vAuditEventsForPolicyEditAndDuplicate 这两个表，创建包含这些额外数据的报告。

1. 从现有的数据源创建新的查询，如从现有的数据源创建查询 （第 15 页）中所述。
2. 在 Microsoft Query 中，单击 表，然后单击 添加表。在 添加表 对话框中，选择 vAuditEventsForPolicyEditAndDuplicate，然后单击 添加。完成之后，单击 关闭。
3. 通过将两个表中的共同的字段联结起来，从而将这两个表相互联结起来。在第一个表中，单击共同的字段 EventID，用鼠标将它拖到第二个表中的 EventID 字段上。
4. 双击它们，将字段添加到查询中。或者，您可以从表的显示区拖曳字段，将它添加到查询中。

提示
您可以使用 Microsoft Query 中的 连接（表 > 连接）创建一个连接两个表的查询。



5. 要保存查询，请在 文件 菜单中，单击 保存。
6. 要返回 Excel，单击 返回数据 按钮。

或者，在 文件 菜单中，单击 将数据返回到 Excel。

返回 Excel，导入数据 对话框会出现。创建表（创建表 （第 12 页））。PolicyContent 列中将包含 XML 格式的策略配置更改。

提示

如果您使用 Microsoft SQL Server Management Studio，您可以直接查询 Reports.vAuditEventsForPolicyEditAndDuplicate 视图。然后，您在查询结果中的 PolicyContent 列查看某个链接时，策略的内容会在 XML 编辑器中显示，所使用的格式的可读性会比 Excel 表好。

9 会审核哪些操作

会受到审核的操作包括：

- 计算机操作
- 计算机组管理
- 策略管理
- 角色管理
- Sophos Update Manager 管理
- 系统事件

9.1 计算机操作

以下的计算机操作会被审核：

- 承认已知/处置警报和错误
- 保护计算机
- 更新计算机
- 删除计算机
- 执行计算机的完整系统扫描

9.2 计算机组管理

针对组管理所记录的操作有：

- 创建组
- 删除组
- 移动组
- 重命名组
- 指派计算机到组

9.3 策略管理

针对策略理所记录的操作有：

- 创建策略 （第 20 页）
- 重命名策略
- 复制策略 （第 20 页）
- 编辑策略
- 指派策略到计算机

- 重置策略为厂商默认值
- 删除策略 （第 20 页）

9.3.1 创建策略

当您创建新策略时，默认策略会被复制到一个名为“新建策略”的新策略中。您可以在这个新建策略创建之后，立即重新命名它。例如，如果您创建了一个新的防病毒和 HIPS 策略，并将它重新命名为“服务器”，那么，以下的审核记录将会被创建：

表 1: 创建新策略，并给与它新的名称。

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	Servers	Success

9.3.2 复制策略

当您复制策略时，会有一个“复制策略”事件被创建，例如：

表 2: 复制策略

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 删除策略

当您删除某个策略时，任何使用了被删除的策略的组，都会恢复使用默认策略。在这种情况下，不会创建单独的，显示重新应用了默认策略的审核事件。

9.4 角色管理

针对角色管理所记录的操作有：

- 创建角色
- 删除角色
- 重新命名角色
- 复制角色
- 添加用户到角色

- 从角色中删除用户
- 添加权限到角色
- 从角色中删除权限

9.5 Sophos Update Manager 管理

针对 Sophos Update Manager 管理所记录的操作有：

- 更新更新管理
- 使更新管理器遵照配置
- 确认已知警报
- 删除更新管理器
- 配置更新管理器

9.5.1 Update Manager 配置中的更改是怎样被记录的？

在 Enterprise Console 中，配置更新管理器 对话框里包含了数个标签页和配置选项，这些配置选项即是更新管理器的配置策略。当您编辑更新管理器的配置时，所做的操作会对照以下策略，记录到日志中：

- 更新管理器 - 预订 - 指定更新管理器保持更新的软件预订。
- 更新管理器 - 上游 - 指定更新管理器的更新源。
- 更新管理器 - 下游 - 指定更新管理器下载软件的共享文件夹。
- 更新管理器 - 计划 - 指定更新管理器检查安全隐患检测数据和软件更新文件的频率。
- 更新管理器 - 常规 - 指定更新管理器的日志记录选项。
- 软件预订 — 指定软件预订的配置，例如，“建议”。

有时，一个更新管理器策略中的更改，会引起其它更新管理器策略发生更改（如：参数 ID 的值的更改）。在这种情况下，您将会在 SophosSecurity 数据库中看到针对您所做的一个更改而生成的数个记录。例如，如果您在 配置更新管理器 对话框中的 计划 标签页中创建一个计划，然后，单击“确定”，那么，以下的审核条目会被创建：

表 3: 创建 Update Manager 的更新计划

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

EventId	Action	Target Type	Target SubType	Target Name	Parameter Type	Parameter Value	Result
20	Edit	Policy	Update Manager - subscription		None		Success

在这种情况下，只有第一个操作，在日志中记录为更新管理器 - 计划策略，会导致真正的配置更改。在日志中记录为此事件的其余的策略更改，是内部的参数 ID 更改。要检查这些更改是什么，您可以使用 SophosSecurity 数据库的 Reports.vAuditEventsForPolicyEditAndDuplicate 视图，如创建 XML 格式的策略更改报告 （第 17 页）中所述。

9.6 系统事件

以下的系统事件会被审核：

- 启用审核
- 禁用审核

10 Sophos Auditing 数据字段

以下数据库视图或数据源，可供 Sophos Auditing 使用：

- Reports.vAuditEventsAll
- Reports.vAuditEventsForPolicyEditAndDuplicate

各个数据源可以使用的数据字段如下所示。所有“日期时间型”栏中的时间都是 UTC 时间，格式为 "yyyy-mm-dd hh:mi:ss"（年-月-日 时：分：秒）（24 小时制）。两种视图都使用的字段以黑体突出显示。

Reports.vAuditEventsAll

Reports.vAuditEventsAll 数据库视图中包含审核事件的完整列表，以及绝大部分的审核信息。

数据字段	数据类型	描述
EventId	integer	事件的唯一的数字 ID。
Timestamp	datetime	记录在事件中的操作发生的时间。
Action	nvarchar(128)	记录在事件中的操作，如创建、编辑、重命名、指派、删除。
TargetType	nvarchar(128)	对象的类型或操作所修改的配置设置的类型，如组、计算机、策略、角色。
TargetSubType	nvarchar(128)	对象的子类型或操作所修改的设置的子类型，视情况而出现。如：被修改的策略的名称，诸如，防病毒和 HIPS 或 Data Control，等等。
TargetName	nvarchar(4000)	对象的名称或操作所修改的设置的名称，如：用户定义的策略或组的名称。
ParameterType	nvarchar(128)	新设置的类型，或指派给目标的新对象的类型。如：对于 Action="重命名" 和 TargetType="策略"，ParameterType="新名称"。对于 Action="指派" 和 TargetType="计算机"，ParameterType="组"。
ParameterValue	nvarchar(4000)	新设置的值，或新对象的值，如：新的用户定义的策略的名称，或指派计算机到其中的新组。
Result	nvarchar(128)	操作的结果；具有值“成功”或“失败”。
UserName	nvarchar(256)	执行操作的用户的名称。
HostName	nvarchar(256)	用户执行操作时所使用的计算机的名称。

数据字段	数据类型	描述
HostIPAddress	nvarchar(48)	用户执行操作时所使用的计算机的 IP 地址。如果服务器和 Enterprise Console 之间的通讯使用的是 IPv6，那么，IPv6 地址会被记录。否则，IPv4 地址会被记录。
ActionId	integer	操作的唯一的数字 ID。
TargetTypeId	integer	目标类型的唯一的数字 ID。
TargetSubTypeId	integer	目标子类型的唯一的数字 ID。
ParameterTypeId	integer	参数类型的唯一的数字 ID。
SubEstateId	integer	子领域的唯一的数字 ID。
ResultId	integer	结果的唯一的数字 ID，1 （成功）或 0 （失败）。
UserSid	nvarchar(128)	用户的安全标识符 。

Reports.vAuditEventsForPolicyEditAndDuplicate

Reports.vAuditEventsForPolicyEditAndDuplicate 数据库视图包含有关策略更改的信息。

数据字段	数据类型	描述
EventId	integer	事件的唯一的数字 ID。
Timestamp	datetime	记录在事件中的操作发生的时间。
Action	nvarchar(128)	记录在事件中的操作。
Result	nvarchar(128)	操作的结果；具有值“成功”或“失败”。
PolicyType	nvarchar(128)	操作所更改的策略的类型，例如：防病毒和 HIPS 或 Web Control。
PolicyName	nvarchar(4000)	用户定义的策略名称。
PolicyContent	XML	XML 格式的策略配置更改脚本。
UserName	nvarchar(256)	执行操作的用户的名称。

11 排疑解难

如果 Sophos Auditing 不能工作，会有一个来源为 "Sophos Auditing" 的事件记录到“Windows 应用程序事件日志”中。在数据库的连接有问题时，常常会出现这种情况。

12 附录：数据字段值的数字 ID

以下表格显示某些 Sophos Auditing 数据字段值的唯一的数字 ID。

如果您想要绑定任何外部逻辑到导出的审核数据上，我们建议使用这些数字 ID，而不使用字符串值。这有助于避免将来发布 Enterprise Console 时，由于任何字符串的更改，而可能产生的兼容性问题。

数据字段	数据字段值	数字 ID
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
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

数据字段	数据字段值	数字 ID
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
	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

数据字段	数据字段值	数字 ID
Result	Pending	0
	Success	1
	Failure	2

13 技术支持

您可以通过以下各种方式获得 Sophos 产品的技术支持：

- 访问 community.sophos.com/ 的 Sophos Community 论坛，并搜索遇到相同问题的其它用户。
- 访问 www.sophos.com/zh-cn/support.aspx 的 Sophos 技术支持知识库。
- 在 www.sophos.com/zh-cn/support/documentation.aspx 中下载产品的技术文档。
- 访问 https://secure2.sophos.com/support/contact-support/support-query.aspx 联系我们的技术支持团队。

14 法律声明