

# Lepide Sharepoint服务器审计

## Lepide Sharepoint服务器审计

概述

要求和前提条件

审计SharePoint的前提条件

在SP服务器上安装Microsoft CLR Types

在SP服务器上安装SQL Management Objects所需用户权限

服务的权利

本地系统权限

审计数据库所需的SQL Server权限

所需的端口

添加SharePoint组件

SharePoint服务器详细信息安装SharePoint审计代理站点收集设置

数据库设置

## 概述

Lepide数据安全平台提供了一种全面的方式，可以跨Active Directory、组策略、Exchange on-premises、Microsoft Office 365、SharePoint、SQL Server、Windows File Server、NetApp Filer和每个可以提供与syslog和RestAPI集成的平台提供可见性。

本指南将带您完成Lepide数据安全平台的SharePoint的标准配置过程。有关安装的信息，请参阅我们的安装和先决条件指南。

如果您在此过程中有任何问题，您可以联系我们的支持团队。联系方式列在本文档的最后。

## 要求和前提条件

### 审计SharePoint的前提条件

以下是添加一个SharePoint Server（任何版本）进行审计的先决条件

- 与SharePoint Server相连的SQL Server实例的连通性和可访问性
- Microsoft System CLR Types for SQL Server2012

- Microsoft SQL Server 2012 Management Objects

- 要监控的服务器和安装软件的计算机上都应安装 .net Framework 4.6。

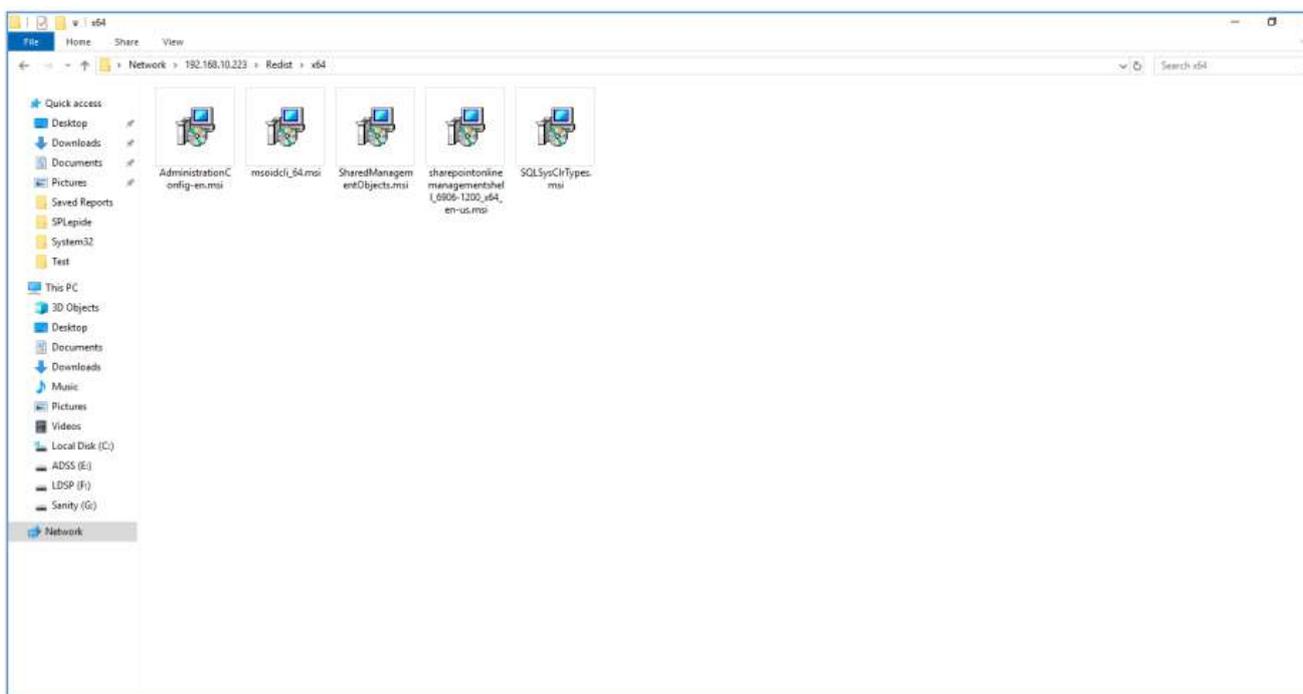
注意：只有在运行SharePoint的服务器计算机上安装了Microsoft System CLR Types for SQL Server 2012和Microsoft SQL Server 2012 Management Objects后，才能在leide Data Security Platform中添加SharePoint Server进行审计。安装这两个附加组件的安装文件随解决方案的压缩安装文件一起提供。

添加用于审计的SharePoint组件所需的用户权限请参见第3节添加SharePoint组件。

## 在SP服务器上安装Microsoft CLR Types

按照以下步骤安装Microsoft System CLR Types for SQL Server 2012:

1. 转到服务器并浏览安装了Lepide数据安全平台的计算机的文件夹。
2. 打开Redist文件夹，其中有不同的文件夹。“x64”文件夹包含64位Windows Server操作系统的安装文件，“x86”文件夹包含32位Windows Server操作系统的安装文件。
3. 打开所需的文件夹。



4. 将这些文件复制到SP服务器并运行安装文件SQLSysClrTypes。安装Microsoft System CLR Types for SQL Server 2012。

如果在将安装文件复制到本地文件系统后运行安装文件，则不会出现警告消息。

5. 单击Run。它显示Windows安装程序。

6. 初始化Windows Installer后，它会显示安装向导。

7. 单击Next。下一步显示Microsoft Corporation的许可协议。

8. 请仔细阅读许可协议。安装Microsoft CLR类型的许可和条款将在您和Microsoft之间进行。如果同意，则单击“我接受许可协议中的条款”。

9. 单击Next继续。模块现在可以安装了。

10. 单击Install开始安装。

11. 一旦安装了Microsoft System CLR Types, 向导中就会出现成功的消息。

12. 单击Finish完成该过程并关闭向导。

## 在SP服务器上安装SQL Management Objects

按照以下步骤安装Microsoft SQL Server 2012 Management Objects Setup。

1. 转到服务器并浏览安装了leide数据安全平台的计算机的文件夹。
2. 打开Redist文件夹, 其中包含两个子文件夹。"x64"文件夹包含64位Windows Server操作系统的安装文件, "x86"文件夹包含32位Windows Server操作系统的安装文件。
3. 打开所需的文件夹
4. 将这些文件拷贝到SP服务器上, 运行安装文件sharedmanagemenobjects。安装SQL管理对象。
5. 单击Run。它显示Windows安装程序。
6. 初始化Windows Installer后, 它会显示安装向导。
7. 单击Next。下一步显示MicrosoftCorporation的许可协议。
8. 请仔细阅读许可协议。安装Microsoft SQL Server 2012 Management Objects的许可将在您和Microsoft之间进行。如果您同意, 请单击"我接受许可协议中的条款"。
9. 单击Next继续。模块现在可以安装了。
10. 单击Install开始安装。
11. 一旦安装了SQL Management Objects, 向导中就会出现成功的消息。
12. 单击Finish完成该过程并关闭向导。
13. 关闭Redist文件夹。

## 所需用户权限

要安装和使用Lepide数据安全平台, 您需要对将要安装它的系统拥有适当的权限。此外, 您还需要具有访问Active Directory、Exchange Server、SQL Server和SharePoint Server的适当权限。

### 服务的权利

安装完成后运行Lepide数据安全平台服务, 可选择以下对象或用户。

- 本地系统管理员
- Domain Admins Group成员

### 本地系统权限

在安装解决方案的本地计算机上, 用户应具有以下权限:

- 对安装操作系统的驱动器具有完全访问权限
- 在注册表中具有读/写权限按照以下步骤分配这些权限。

1. 转到控制面板, 选择用户帐户。

2. 选择User并选择Change Account Type。
3. 将用户设置为Administrator。
4. 单击Save。

注意：

1. 上述步骤可能因系统安装的Windows版本而异。
2. 如果系统中不存在“User Account”，请创建一个具有“administrator”权限的“User Account”。

## 审计数据库所需的SQL Server权限

所提供的用于创建或访问审计日志数据库的用户应该在SQL Server中使用分配的sysadmin角色登录。

如果您正在使用Windows身份验证，那么当前登录的Windows用户的登录应该存在于SQL Server中。请执行以下步骤。

1. 如果这样的用户登录还不存在，那么按照下面的步骤创建它。
  - a. 打开SQL Server Management Studio。
  - b. 选择“SQL”或“Windows身份验证”。
  - c. 输入SQL Server Administrator的用户名和密码。
  - d. 单击“连接”。
  - e. 在左侧树状面板中，选择“Security→login”。
  - f. 右键单击“登录”，选择“新登录”。
  - g. 登录-新向导出现在屏幕上。
  - h. 输入与当前正在运行莱德数据安全平台的登录用户相同的登录名。
  - i. 进入“Server Roles”，选择“sysAdmin”。
  - j. 单击“确定”。
2. 如果用户存在，但是没有分配这样的权限，那么按照以下步骤分配所需的权限。
  - a. 打开SQL Server Management Studio。
  - b. 选择“SQL”或“Windows身份验证”。
  - c. 输入SQL Server Administrator的用户名和密码。
  - d. 单击“连接”。
  - e. 在左侧树状面板中，选择“Security→login”。
  - f. 展开“登录”，选择需要登录的用户。
  - g. 右键单击用户，选择“属性”。
  - h. 进入“Server Roles”，选择“sysAdmin”。
  - i. 单击“确定”。
  - j. 进入“状态”页面，选择“授予”和“启用”。

k. 单击“确定”。

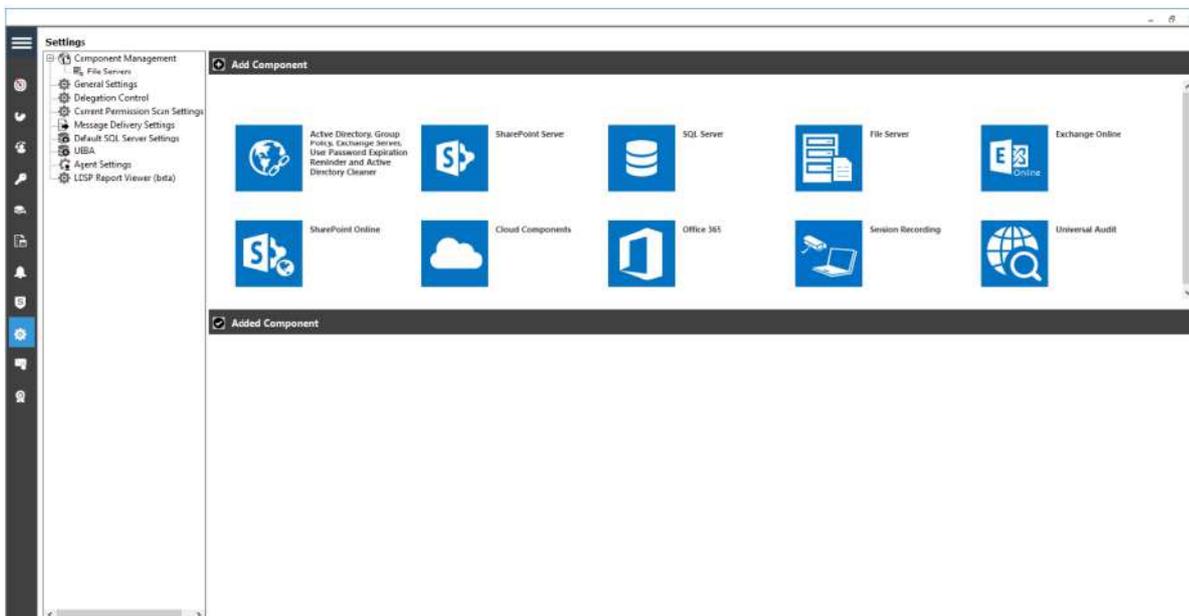
## 所需的端口

本软件使用的端口有以下几种：

1. Lepide数据安全平台使用以下端口进行通信：
  - a. ldapquery使用389端口和636端口。
  - b. RPCSS（远程过程调用服务）的445端口
  - c. 与事件日志通信的135端口
  - d. 远程PowerShell通信的TCP/5985（HTTP）和TCP/5986（HTTPS）
  - e. SQL Server通信的默认端口。在大多数情况下，SQL的默认端口是1433。
2. 本解决方案使用了以下微软函数，它们使用不同的端口：
  - a. OpenEventLog（445端口和135端口）
  - b. readdeventlogt（445端口和135端口）
  - c. AdsOpenObject（389端口和636端口）
3. Lepide数据安全平台Web控制台使用7778端口(HTTP)。您可以修改PortNumber。
4. Lepide数据安全平台应用程序使用端口1051。

## 添加SharePoint组件

在继续之前，请确保满足添加SharePoint Server的先决条件。要了解更多的先决条件，请参见2.1审计SharePoint的先决条件。要添加SharePoint组件，在“组件管理”窗口的“添加组件”部分，单击“SharePoint服务器”图标，将该组件添加到解决方案中。



将启动“添加SharePoint服务器”向导：

SharePoint Details

Central Administration URL   
Please add the Central Admin URL correctly.  
Use Format http://ServerName:Port

IP Address

User Name

Password

SQL Server Details

SQL Server Name  ...

Authentication Type

Windows Authentication

SQL Authentication

User Name

Password

Test Connection

< Back Next > Cancel

## SharePoint服务器详细信息

1. 这个步骤有两个部分：

- a) SharePoint详细信息:在SharePoint详细信息部分，你需要提供中央管理URL，IP地址，用户名和密码。以这种格式提供用户名-域\用户或工作组\用户

以下说明提供了有关所需用户权限的进一步信息：

10. 注意：Active Directory中所需的用户权限选择的用户应该是Administrators和Domain Admins组的成员。此外，登录到运行SharePoint和审计代理的计算机的用户应该是域管理员组的成员。  
如果用户没有这些权限，请按照给定的步骤分配权限：

1. 转到管理工具。

2. 打开Active Directory用户和计算机。

3. 选择“用户属性”。

4. 单击“属于”。

5. 单击“添加组”。

6. a. 管理员

b. 域管理员

7. 选择“组”。单击Apply和OK。

SharePoint所需的用户权限选择的用户应该是SharePoint中的Farm Administrator Group的成员。执行以下步骤在“场管理员组”中添加用户。

a. 进入“中央管理→安全”。

b. 单击“用户”下的“管理场管理员组链接”。

c. 检查所选用户是否已添加到“机场管理员组”中。

d. 如果此处未列出所选用户，单击“新建”。

e. 在共享“中央管理”弹出框中，键入用户名。一旦输入，SharePoint服务器将识别该名称并显示一个列表。

f. 在弹出的列表中选择用户名。

g. 单击“共享”，将用户添加到“机场管理员”组中

1. 所选用户必须对要审计的每个站点集具有管理权限。为此，用户要么应该是站点集合管理员，要么应该完全控制Web应用程序。

a. 在“Site Collection Administrators”中添加用户。

- i. 在浏览器中打开需要开启审计的Site Collection。
- ii. 单击右上角的“设置”图标，然后单击“站点设置”。
- iii. 在“站点设置”中，单击“用户和权限”下的“站点收集管理员”。
- iv. 检查所选用户是否被列为“站点收集管理员”。

- v. 如果未列出，请添加用户。

如果要启用对将来创建的新站点的审计，请在创建新站点时将所选用户添加为“主站点收集管理员”或“辅助站点收集管理员”。

b. 执行以下步骤，分配“对Web应用程序的完全控制”。

- i. 进入“中央管理→应用程序管理→ManageWeb应用程序”。
- ii. 选择所需的Web应用程序。
- iii. 单击功能区上的用户策略按钮。
- iv. 选择“所有区域”，单击“下一步”。
- v. 选择“完全控制-完全控制”，单击“下一步”。
- vi. 单击“完成”，完成设置。

一旦分配了这些权限，用户就获得了Web应用程序中每个站点集合的管理权限。

本地安全策略所需用户权限选择的用户需要在“本地安全策略”的“以服务方式登录”的安全权限中添加。如果用户没有此权限，则按照以下步骤在安装了SharePoint Server的服务器计算机上分配相同的权限。

1. 转到管理工具→本地安全策略。

2. 在左侧面板中，选择“安全设置→本地策略→用户权限分配”。它在右面板中显示不同的策略。

3. 选择Log on as a service，双击它来访问它的属性。

4. 确保所选用户列在属性窗口的本地安全设置选项卡中。

5. 如果未添加所选用户，则单击“添加用户或组”按钮。它显示选择对象对话框。

SP SQL Server所需用户权限要求SQL Server for SharePoint Content Database中已存在以“Windows认证”身份和sysadmin角色登录的SharePoint用户。

案例1: 如果用户登录还不存在，那么按照下面的步骤创建它。

1. 打开SQL Server Management Studio。

2. 选择SQL或Windows身份验证。

3. 如果是SQL Authentication，请输入SQL Administrator的用户名和密码。

4. 单击连接。
5. 在左边的树状面板中，转到安全→登录。
6. 右键单击“登录”并选择“新登录”。
7. 登录-新向导出现在屏幕上。
8. 输入与要添加SharePoint Server进行审计的SharePoint用户相同的登录名。
9. 切换到“服务器角色”。
10. 同时选择sysAdmin和dbcreator角色。
11. 单击OK。

情况2: 如果用户存在，但是没有分配这样的权限，那么按照以下步骤分配所需的权限:

1. 打开SQL Server Management Studio。
2. 选择SQL或Windows身份验证。
3. 如果采用SQL身份验证，请输入SQL Server管理员的用户名和密码。
4. 单击连接。
5. 在左边的树状面板中，转到安全→登录。
6. 展开login并选择所需的用户。
7. 右键单击用户并选择properties。
8. 切换到“服务器角色”。
9. 同时选择sysAdmin和dbcreator角色。
10. 单击OK。

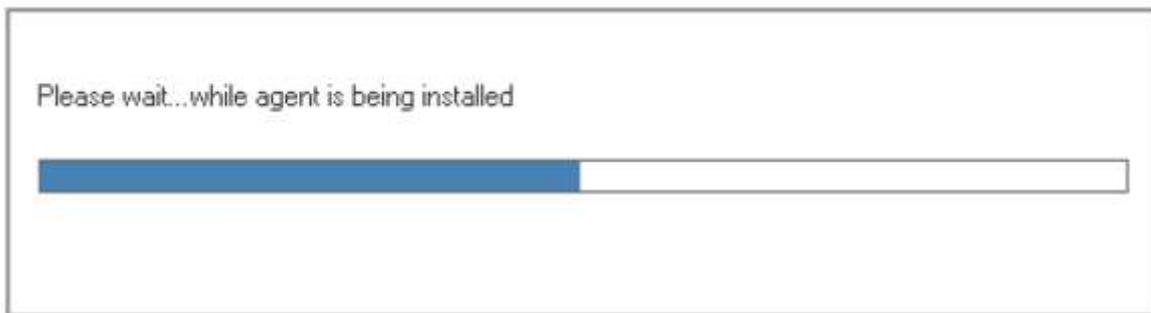
b) "SQL Server详细信息": 手动输入"SQL Server名称"或单击图标枚举所有本地和远程SQL Server, 然后从列表  
中选择一个。

选择身份验证类型并为用户提供凭据。

1. 单击"测试连接"按钮以检查是否成功连接到SQL Server。
2. 单击Next。

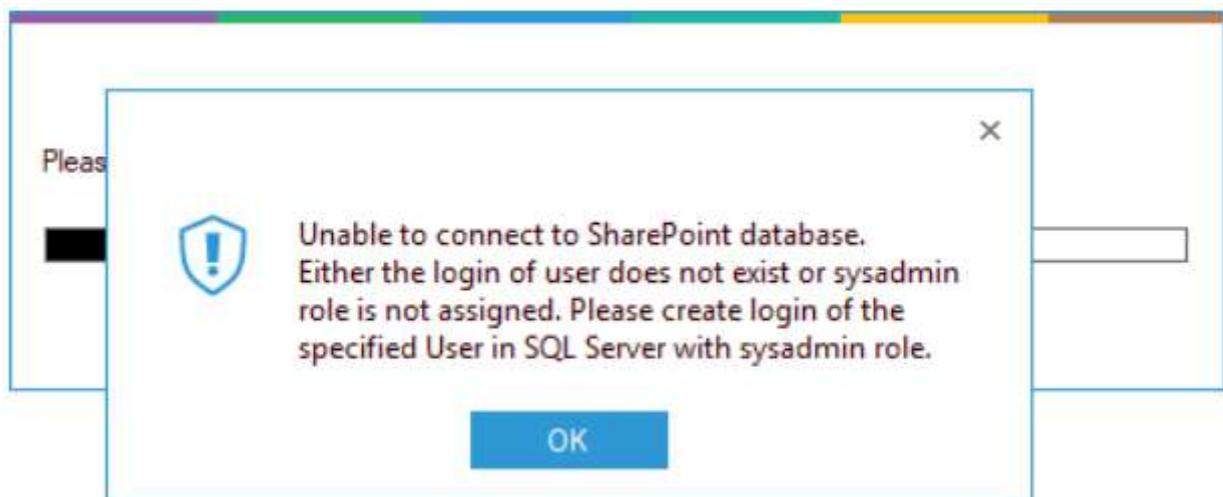
## 安装SharePoint审计代理

解决方案开始在SharePoint Server上安装代理进行审计。

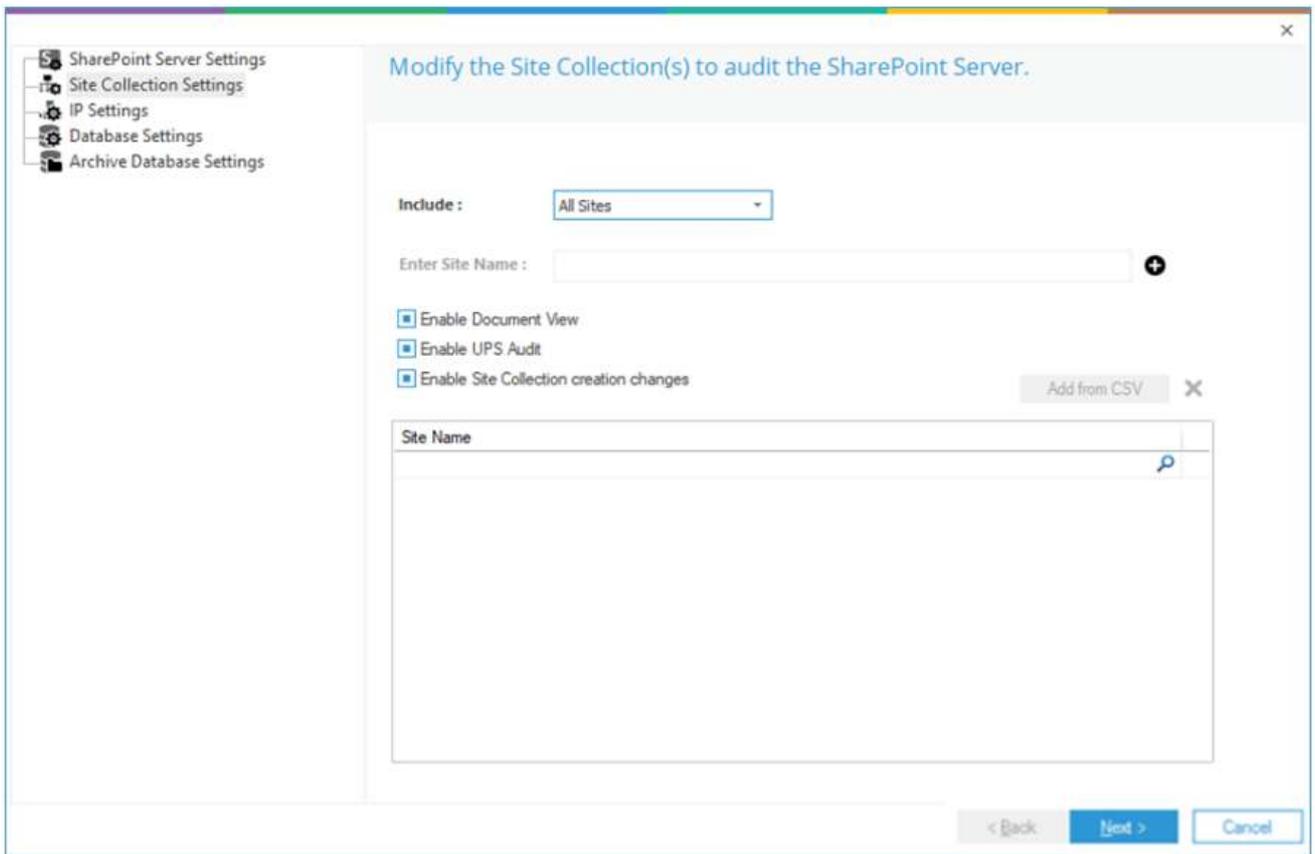


注意: 如果您没有在服务器上安装Microsoft System CLR Types for SQL Server 2012和Microsoft SQL Server 2012 Management Objects Setup, 则在此阶段可能会收到错误。从程序安装文件夹的Redist文件夹安装它们。

注意: 如果在尝试连接到SharePoint时屏幕上出现以下错误, 那么这意味着SharePoint用户的登录不存在, 或者没有分配sysadmin角色给它。



## 站点收集设置



4. 在此对话框中，显示SharePoint上所有站点的列表。您可以选择需要审计的站点。

5. 包括:此下拉菜单有以下选项:

- a. All: 如果要审计所有站点集，请选择此选项。
- b. 排除: 如果要审计除所选SiteCollection之外的所有SiteCollection，请选择此选项。
- c. 包括: 如果要审计所选的站点集，请选中此选项。

按照以下步骤选择站点名称:

- a. 选择包含或排除选项使您能够选择要进行审计的站点。
- b. 如果需要直接添加站点名称，单击图标，在“站点名称”框中输入站点名称。
- c. 单击图标，根据下拉框中选择的站点，勾选需要包含或排除的站点。

6. 为了减少返回的数据集数量，您可以取消选中以下一个或多个复选框:

启用文档

查看启用UPS审计

启用站点数据集创建更改

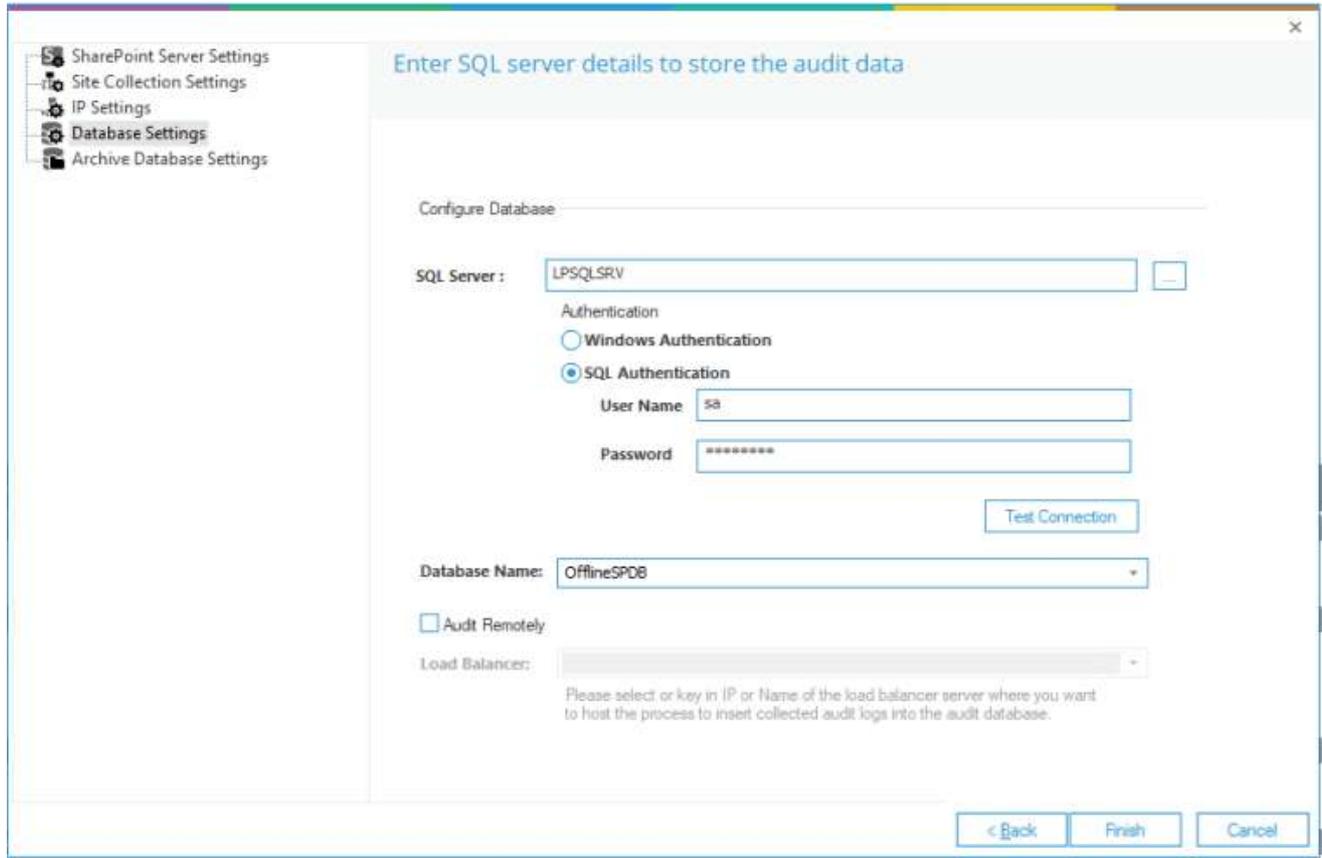
7. 单击“确定”。如果是从CSV文件添加，单击“从CSV添加”，在列表中选择CSV文件。

8. 单击Next。

系统弹出“数据库设置”对话框。

## 数据库设置

在此步骤中，您需要提供将用于存储审计数据的SQL Server和数据库的详细信息。该解决方案允许您连接到本地托管或网络SQL Server。



The screenshot shows a configuration window titled "Enter SQL server details to store the audit data". On the left, there is a navigation pane with "Database Settings" selected. The main area contains the following fields and options:

- SQL Server:** LPSQLSRV
- Authentication:**  Windows Authentication,  SQL Authentication
- User Name:** sa
- Password:** [masked]
- Test Connection:** [button]
- Database Name:** OfflineSPDB
- Audit Remotely:**
- Load Balancer:** [dropdown menu]

Below the Load Balancer dropdown, there is a note: "Please select or key in IP or Name of the load balancer server where you want to host the process to insert collected audit logs into the audit database." At the bottom right, there are buttons for "< Back", "Finish", and "Cancel".

手动输入SQL Server名称或单击按钮显示网络上的所有SQL Server。提供SQL Server用户名和密码，以允许解决方案使用这些凭据访问SQL。

注意：此处选择的用户在SQL Server中应该具有dbcreator角色。

必须测试解决方案与所选SQL Server之间的连接。这有助于验证数据库连接。

- 单击“测试连接”。

如果连接失败，它将显示一个错误，或者显示以下消息，确认连接成功。



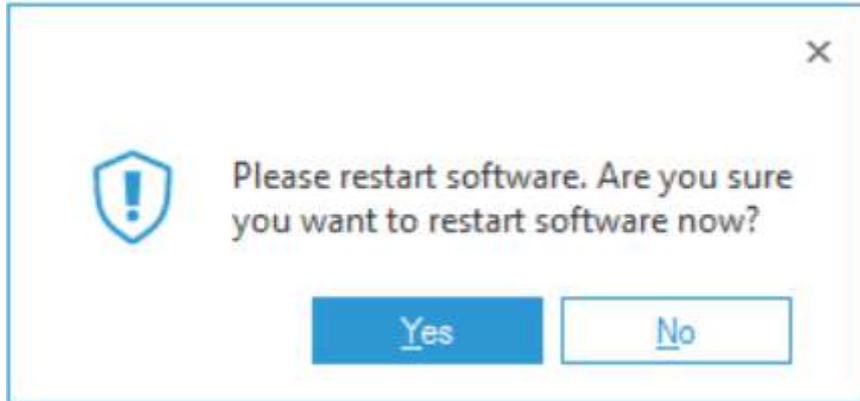
提供数据库名称，Lepide数据安全平台将在其中存储审计日志。

注意：Lepide数据安全平台连接到解决方案本身创建的数据库。当您尝试使用现有数据库时，解决方案会发出警报

如果您是第一次使用该解决方案，您可以为将使用该解决方案创建的新数据库提供一个名称。在重新安装的情况下，您可以使用解决方案先前创建的数据库。

远程审计：选中此复选框后，您可以指定一台服务器来承载将收集的审计日志插入审计数据库的进程。

单击Finish



**HongKe**

虹科

虹科电子科技有限公司

www.haacst.com  
network@hkaco.com

广州市黄埔区开泰大道30号佳都PCI科技园6号楼1-7层

T (+86) 400-999-3848  
M (+86) 135 3349 1614

各分部：广州 | 成都 | 上海 | 苏州 | 西安 | 北京 |  
台湾 | 香港 | 日本 | 韩国 | 美国硅谷

版本：V1.0 - 23/09/10



联系我们



获取更多资料



haacst.com