Lepide Windows文件服务器快速入门指南

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Windows文件服务器的标准配置过程。

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

系统基本要求

• 所需处理器—最低双核处理器—建议四核处理器

• 所需内存—最低4gb内存—建议8gb内存

• 所需磁盘剩余空间—最低1gb—建议2gb

• 以下32位或64位Windows操作系统。

— Windows Server操作系统：2008 R2以上的任何服务器

• 用于存储审计日志的任何SQL Server（本地或网络托管）：
—SQL Server 2005以上的任何SQL Server（标准或企业）

• .NET Framework 4.6及以上版本

支持的审计服务器

审计服务器：Windows文件服务器支持的版本：

· Windows 7 及更新的版本

· Windows Server 2008 R2 及更新的版本

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，您还需要具有访问文件服务器的适当权限。有两种方法来配置Windows文件服务器与Lepide数据安全平台：

• 使用最少权限

• 使用完全权限

注意：要了解这两种方法所提供的功能的差异，请参阅最小特权原则文档。

最小特权

若要以最少权限配置leide数据安全平台，服务帐户需要以下权限：

• 域用户帐户。

• 该帐户应该对SQL数据库具有Db_owner/Db_creator权限。还可以使用具有上述特权的SQL帐户。

• 该帐户应该是文件服务器上本地管理员组的成员。

• 该帐户应该是Lepide服务器上本地管理员组的成员。

• 该帐户应具有列表文件夹/读取数据，遍历文件夹/执行文件和读取权限对要审计的共享的权限。

• 该帐户应用于登录到ide服务器以配置文件服务器进行审计。

• SYSTEM帐户应该对安装代理的文件夹有修改权限。

完整的特权

要以完全权限配置Lepide数据安全平台，服务帐户需要以下权限：

• Active Directory中域管理员组的成员

• 应该有权访问文件服务器上的admin$

SQL Server必备权限

• 对于Windows身份验证：当前登录的Windows用户必须在SQL Server中存在，并且在SQL Server中指定的角色为dbcreator。

• 对于SQL身份验证：具有dbcreator权限的本地SQL帐户。

注意：使用SQL身份验证时，应将SQL服务器设置为混合身份验证模式。

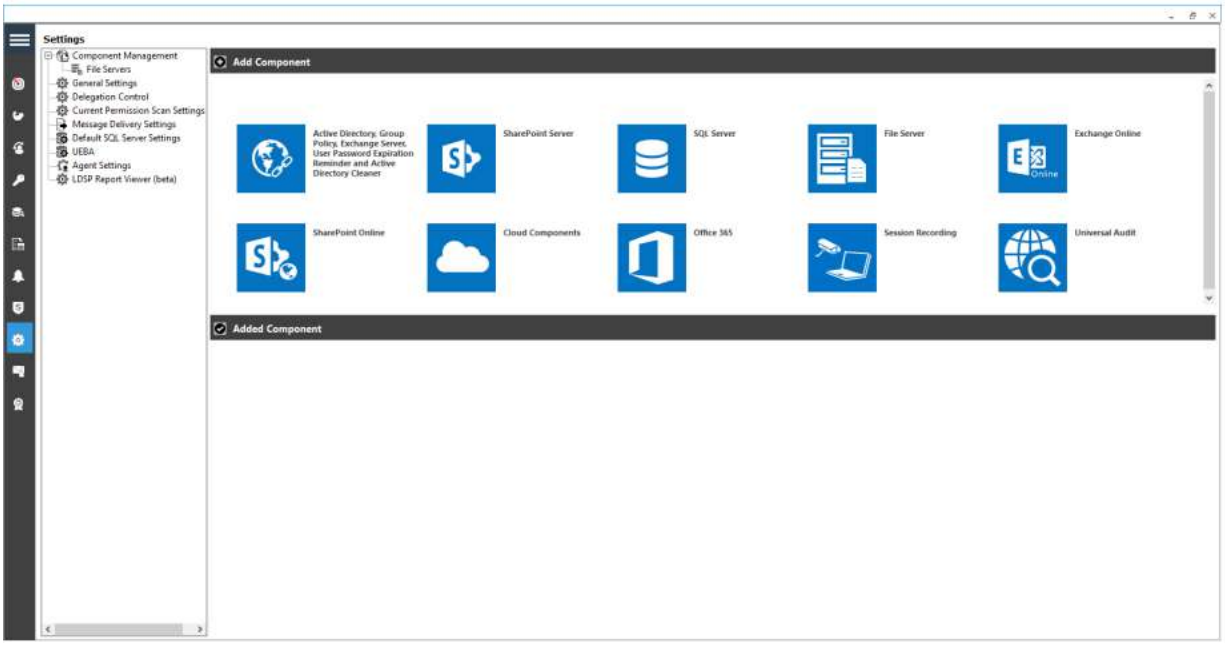
所需的端口

本软件使用以下端口用于不同目的。

1. Lepide数据安全平台使用以下端口进行通信：
   a. LDAP查询使用389端口和636端口。
   b. rpc(远程过程调用服务)的445端口
   c. SQL Server通信的默认端口。在大多数情况下，SQL的默认端口是1433。
   d. 文件服务器与leide应用服务器之间的数据传输端口为3000。
2. Lepide数据安全平台Web控制台使用7778端口（HTTP）。
3. Lepide数据安全平台应用程序使用端口1051。

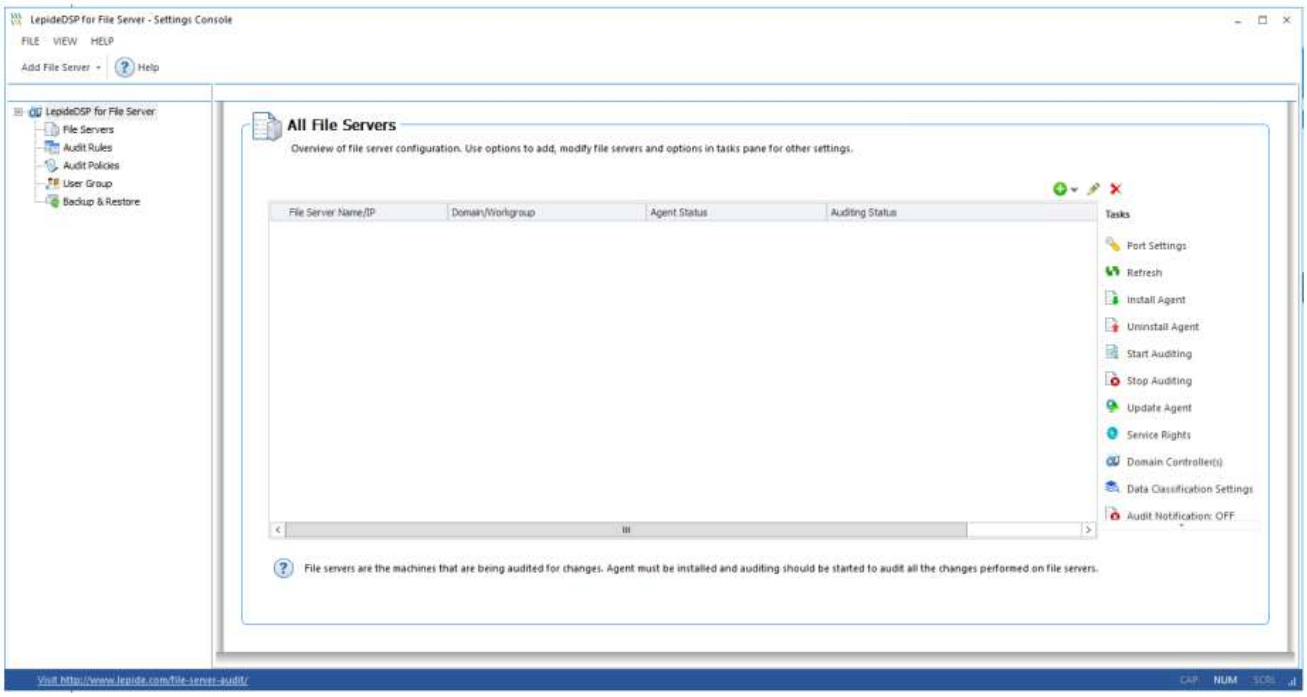
添加Windows文件服务器

在安装解决方案并将Lepide服务配置为使用管理凭据运行之后，可以添加用于审计的Windows文件服务器。



1. 在Component Management窗口的Add Component部分下，单击File Server图标，将该组件添加到解决方案中。

系统弹出"文件服务器设置控制台"对话框：

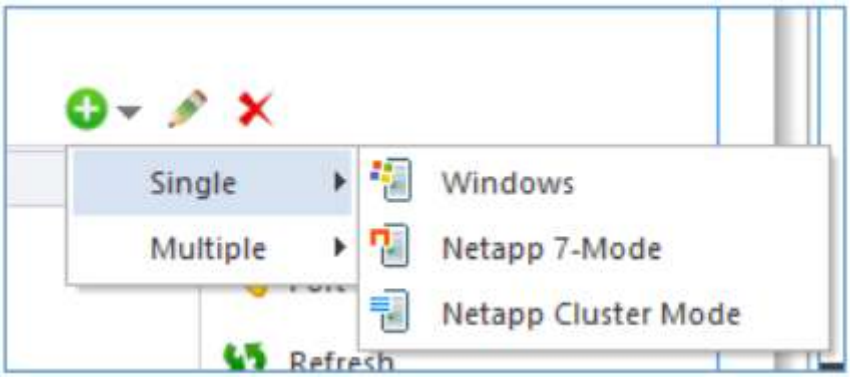


2. 单击工具栏上的"添加文件服务器"图标，可以添加以下文件服务器：

• Windows文件服务器

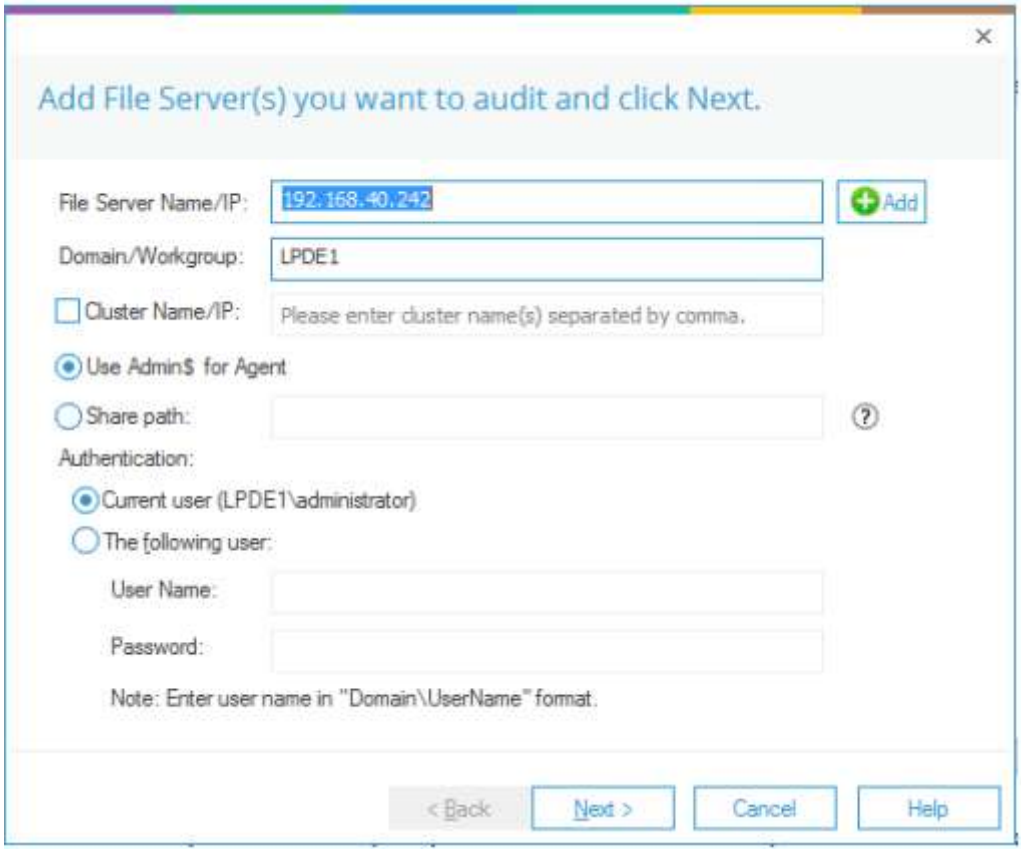
• NetApp文件服务器

单击添加文件服务器图标，选择单个，然后选择Windows。



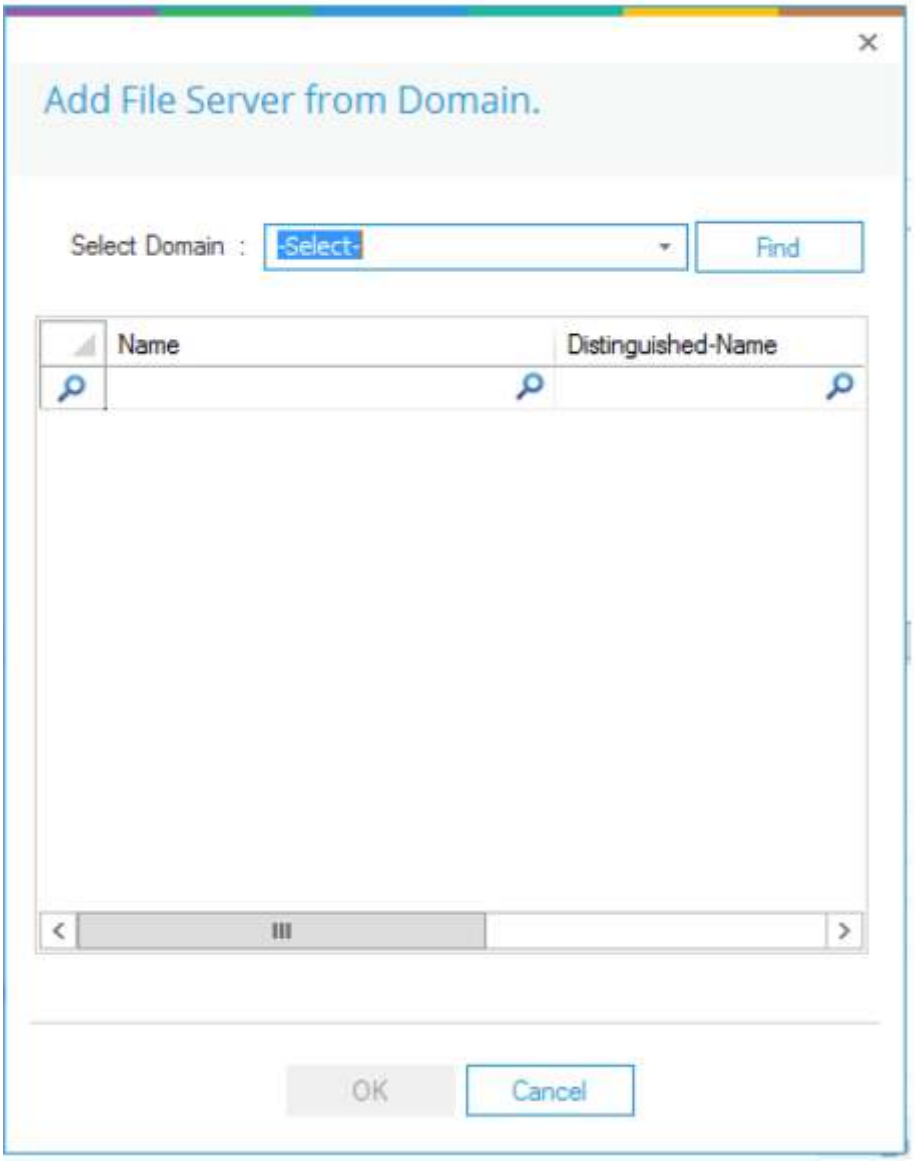
注意：本指南只解释了添加单个windows文件服务器的过程。要添加多个文件服务器，请参考我们的高级Windows文件服务器配置指南。

3. 启动"添加文件服务器"向导。

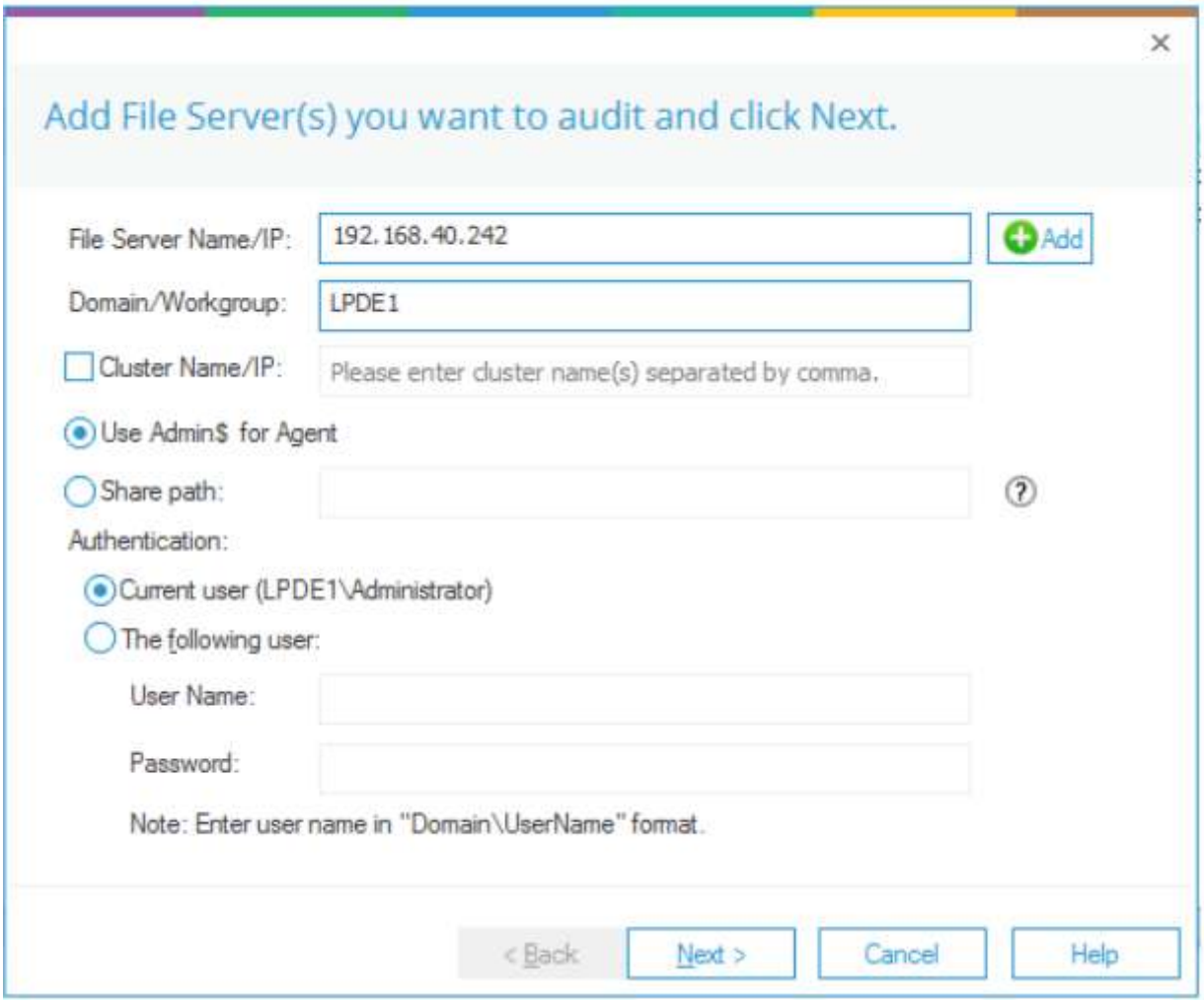


4. 输入服务器的名称或IP地址及其域或工作组名称。

5. 您可以单击"添加"按钮扫描域网络并选择所需的文件服务器，而不是手动输入。

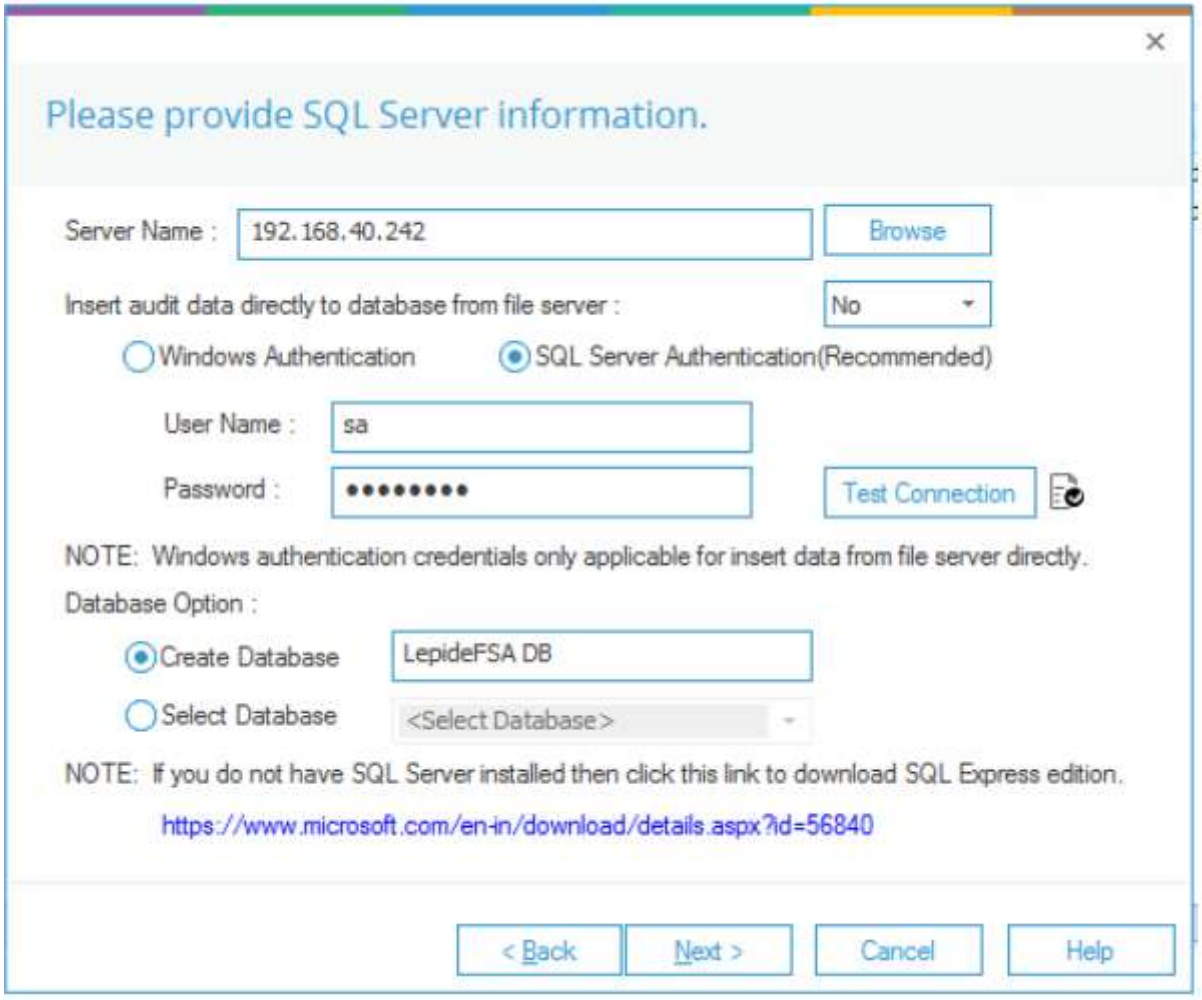


6. 在"选择域"窗口中键入域的名称。
7. 单击"查找"按钮以在空白区域中列出其计算机。
8. 选择要审计的计算机并单击"确定"。它将带您回到前面的向导，该向导现在显示所选的File Server。
9. 选择要向其添加文件服务器的用户。
10. 如果您以具有上述权限的用户身份登录，则可以选择"当前用户"。
11. 如果登录的用户没有所需的权限，则必须选择以下用户选项并提供具有所需权限的用户的登录凭据。



12. 输入详细信息后，单击Next。

13. 下一步是提供SQL Server的详细信息：



14. 如果从文件服务器到SQL服务器的1433端口没有打开，请将"从文件服务器直接插入审计数据到数据库"选项设置为NO。

15. 输入"服务器名称"或单击"浏览"选择所需的SQL Server。

16. 有两个身份验证选项：

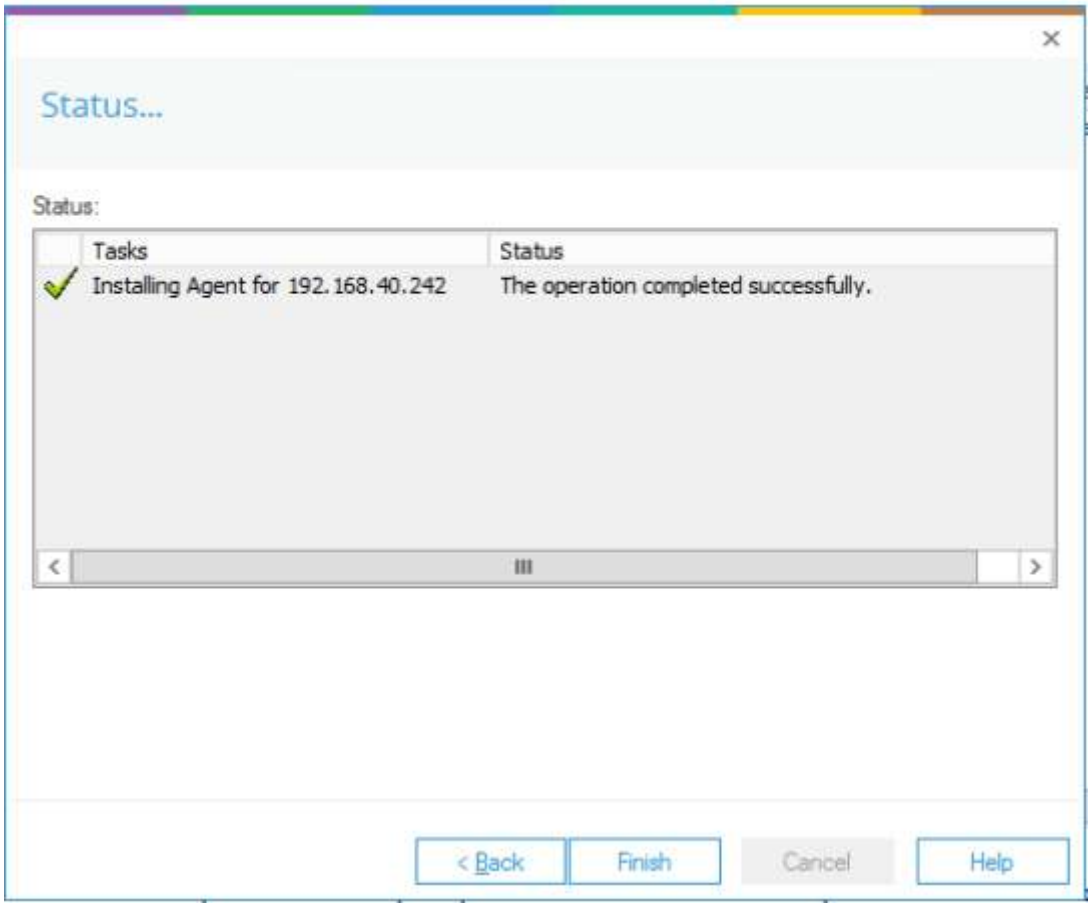
    • Windows身份验证：请输入在SQL服务器上至少具有所有者权限的域帐户。

    • SQL Server身份验证：如果SQL Server安装在远程机器或本地机器上，请选择此模式。我们建议选择此选项。提供SQL用户的用户名和密码，该用户具有创建新数据库的足够权限。

17. 在Create database字段中输入数据库名称以创建新数据库或将其保留为默认值。您还可以选择由Lepide或其他应用程序创建的现有数据库。

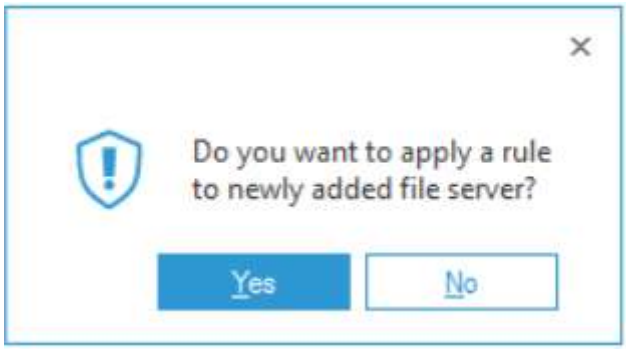
18. 单击Next开始在Windows File Server上安装审计代理。

安装完成后，系统弹出如下对话框：

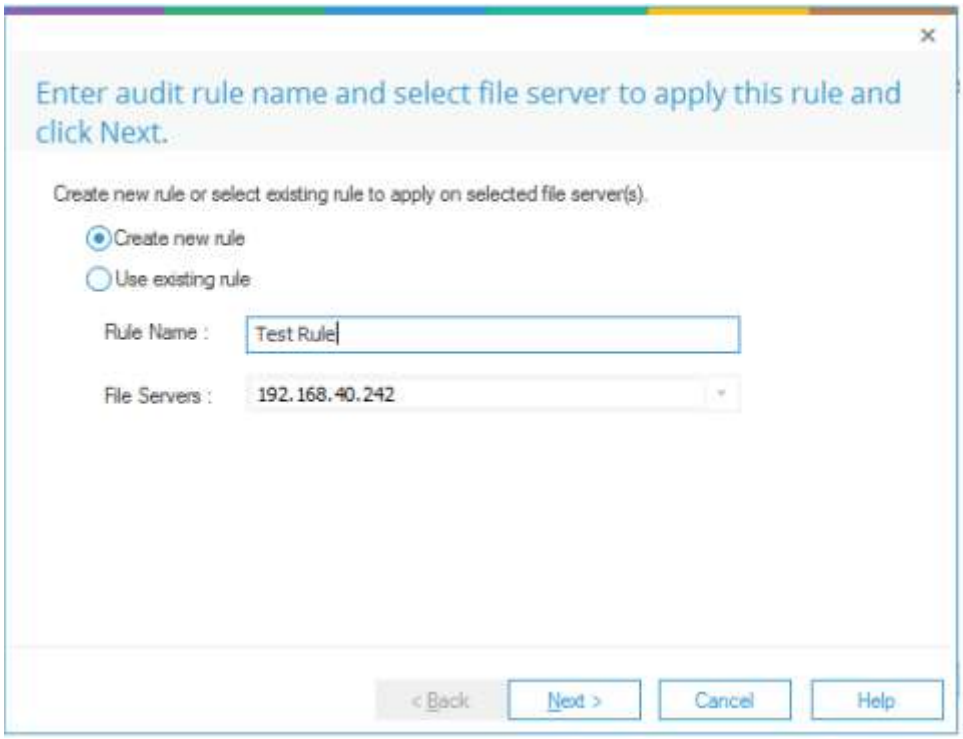


19. 单击Finish完成该过程。

弹出对话框，询问是否将规则应用于新添加的文件服务器。

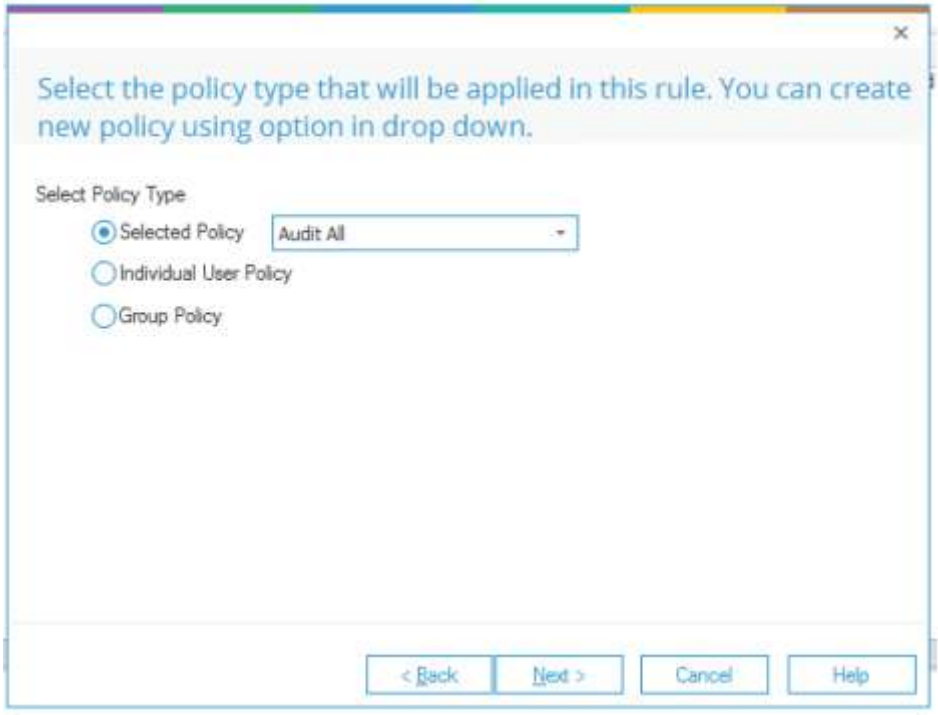


20. 单击Yes并在下一个窗口中创建一个新规则。



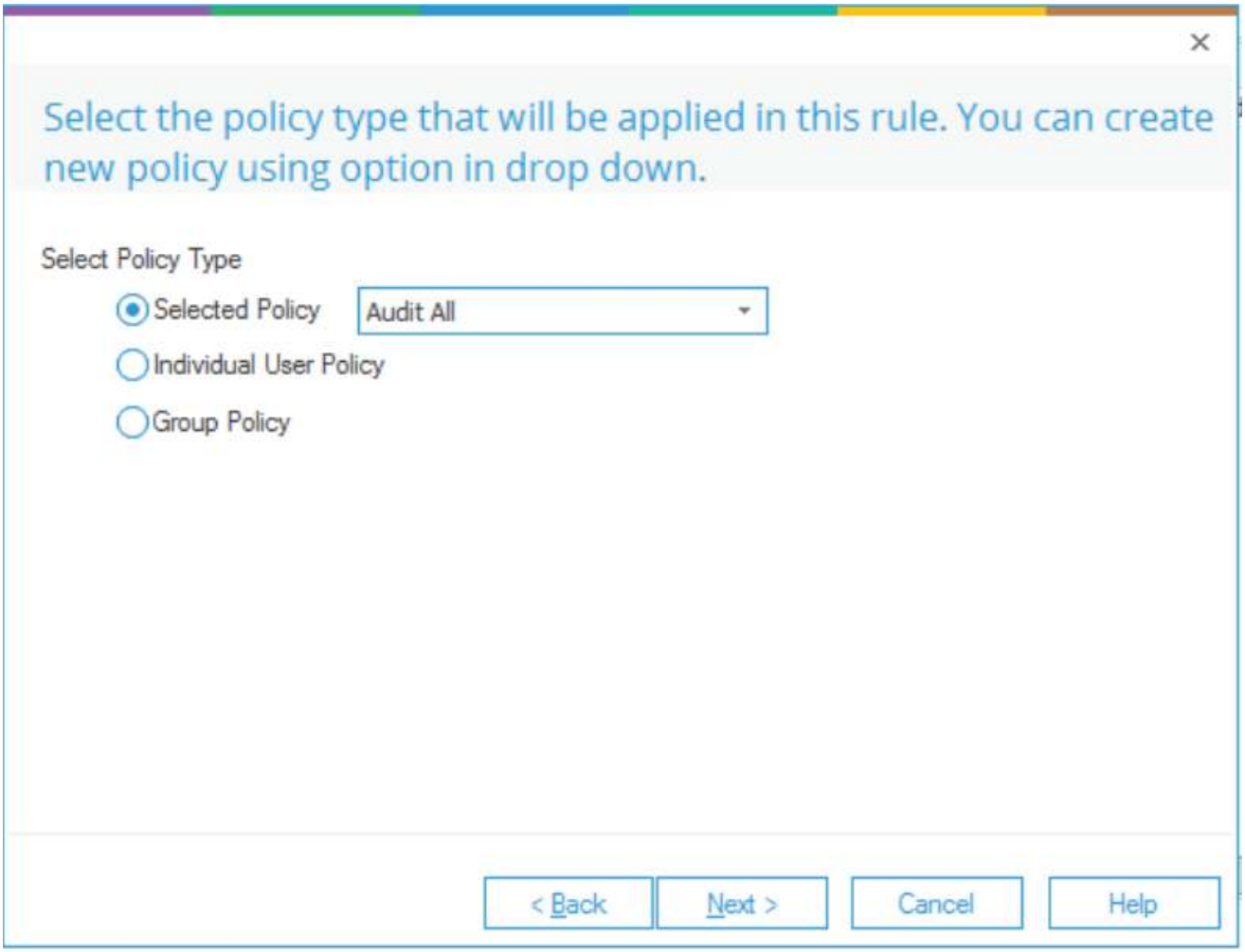
21. 输入规则名称，并选择要为其创建规则的文件服务器（如果该文件服务器尚未在"文件服务器"下拉菜单中选中）。

22. 单击Next，系统弹出"审计策略"对话框：

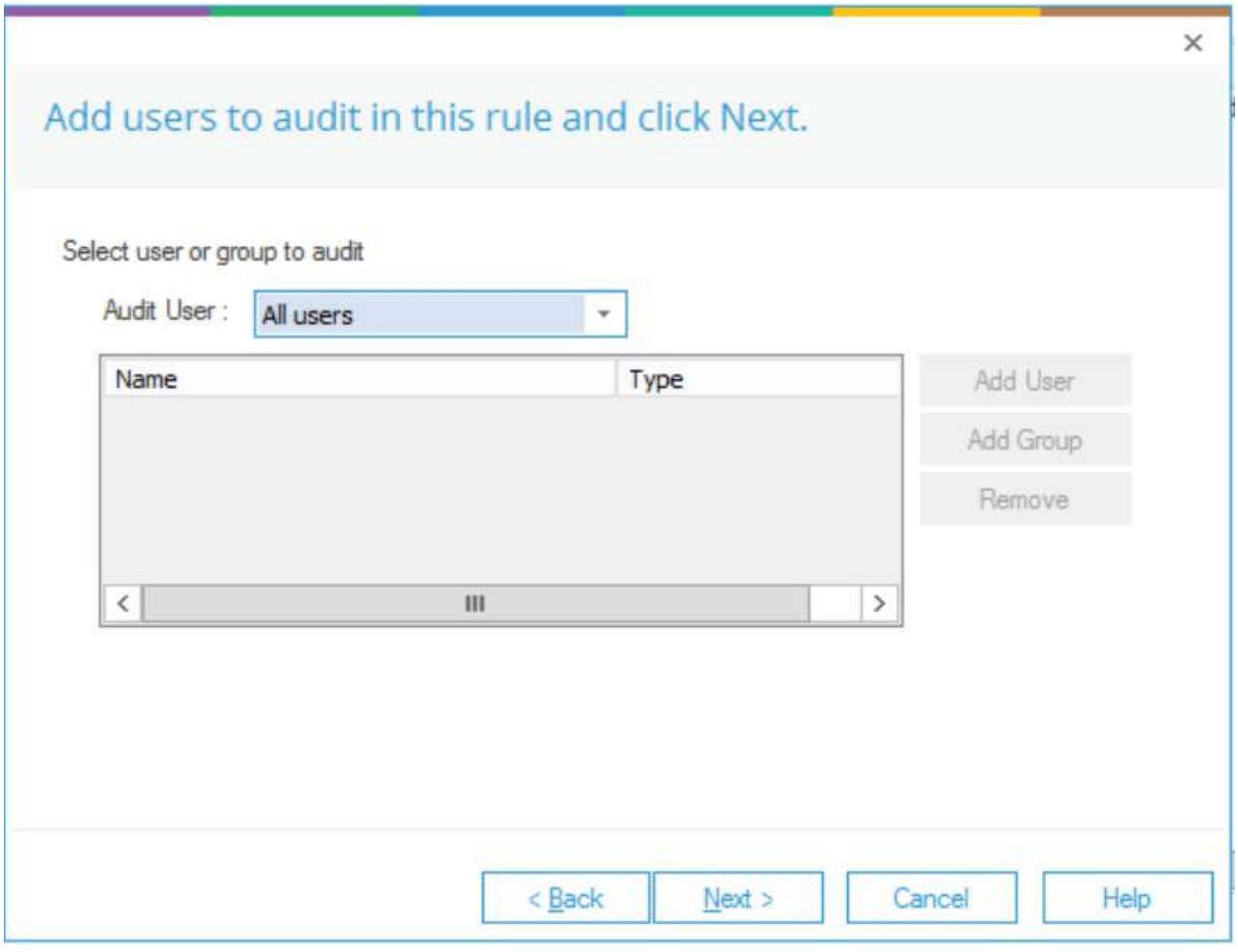


注意：在本例中，我们将创建一个具有预定义策略的审计规则。如需创建用户自定义策略的审计规则，请参见《高级文件服务器配置指南》

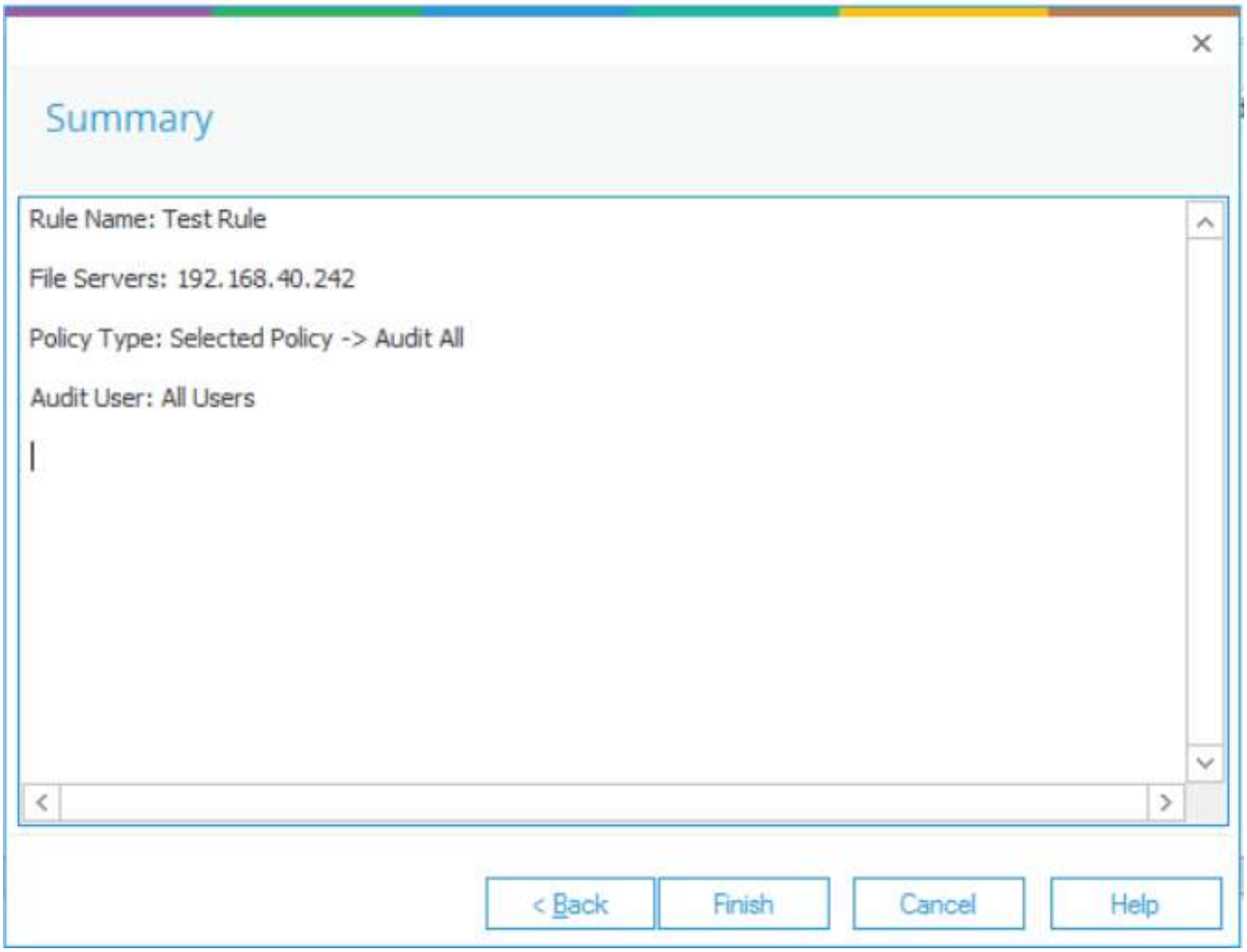
对于本例，我们将选择Audit All策略：


Select the policy type that will be applied in this rule. You can create new policy using option in drop down.
Select Policy Type
Selected Policy
Audit All
Individual User Policy
Group Policy
< Back
Next >
Cancel
Help

23. 单击Next


Add users to audit in this rule and click Next.
Select user or group to audit
Audit User :
All users
Name
Type
Add User
Add Group
Remove
< Back
Next >
Cancel
Help

24. 在“审计用户”页签中选择“所有用户”，单击“下一步”。在这种情况下，规则应用于所有用户。
25. 单击“Next”，弹出“Summary”对话框。



26. 单击Finish完成该过程。新增的审计规则显示在列表中。

27. 单击所有文件服务器上的更新代理以应用新的设置通知，并按照屏幕上的说明更新代理。

28. 创建审计规则后，重新启动主控制台，并转到主面板中的Audit Reports选项卡查看报告。

注意：每次更改应用的审计规则时，都需要更新代理。如果不这样做，审计将不会更新，并且报告在生成时将不包含新的修改。