

Lepide Microsoft SQL SERVER基本配置

Lepide Microsoft SQL SERVER基本配置 概述 要求和前提条件 系统基本要求 支持的审计服务器所需用户权限SQL Server必备权限 所需端口

添加SQL Server 添加SQL Server快速配置 SQL Server详细信息 数据库设置执行以下步骤配置数据库设置。添加SQL Server高级配置

> SQL运行状况监视 审计设置 对象设置 用户设置 存档数据库设置

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 onpremises、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Microsoft SQL server的Lepide数据安全平台的标准配置过程。

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

•所需磁盘剩余空间一最低1gb一建议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: Microsoft SQL Servers

支持的版本: Microsoft SQL Server 2005及以上(标准或企业)

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SQL服务器的适当权限。

为了配置Lepide数据安全平台对Microsoft SQL Server进行审计,该服务帐户需要具备以下权限:

• Active Directory中的Domain Admins Group成员。

•该帐户应具有SQL数据库的系统权限。还可以使用具有上述特权的SQL帐户。

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。

所需端口

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。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. WMI (Windows Management Instrumentation)的135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。

2. Lepide数据安全平台Web控制台使用7779端口(HTTP)。

3. Lepide数据安全平台应用程序使用端口1051。

添加SQL Server

添加Microsoft SQL Server操作步骤如下:

											- 8 ×
-	Settings										
_	🕀 🔞 Component Management	Add Compone	ent								
	- En File Servers										
	Delegation Control										
•	Current Permission Scan Settings Message Delivery Settings			-				7			
æ	Default SQL Server Settings	6	Active Directory, Group Policy, Exchange Server,		SharePoint Server	SQL Server		File Server		Exchange Online	
200	- G Agent Settings	(Sol	Reminder and Active	SP					EX		
^	- IDSP Report Viewer (beta)		Contractory Consents	a second the					Contract Contract		
8											
÷.			SharePoint Online		Goud Components	Office 365		Session Recording	1	Universal Audit	
Line .		S>									
۰									10		
S				-			10 a				t
		Added Compo	nent								
0		And a state of the second second second	81/4901								
-											
×											
	C 3										

•在"组件选择"对话框中选择"SQL Server"选项。

			×
Configuration Type			
Please select configuration method.			
Express Configuration			
(Configure the SQL Server with default settings)			
(conligue the sale server with default settings)			
Advanced Configuration			
(Configure the SQL Server each settings individually)			
		A COLUMN	the second second
	< <u>B</u> ack	Next >	Cancel

该解决方案提供了两种不同的方式来添加SQL Server。

- •快速配置:添加SQL Server的最小推荐设置。
- •高级配置:添加SQL Server与高级设置自定义审计。

添加SQL Server快速配置

在"添加SQL Server"向导中执行以下步骤。

- 1. 在向导中选择Express Configuration。
- 2. 单击Next。它要求您提供要添加的SQL Server的详细信息。

SQL Server详细信息

		×
SQL Server Credentials		
Please enter SQL Server Credentials	s to audit	
SQL Server Details		
SQL Server Name	LPSQLSRV	
Authentication Type		
Windows Authent	tication	
 SQL Authentication 	n	
User Name	sa	
Password		
	Test Connection	
	< <u>B</u> ack <u>N</u> ext >	Cancel

3. 该解决方案允许您添加本地或网络SQL Server。您可以在文本框中手动输入SQL Server的名称。或者,您可以 单击该图标在列表中枚举所有SQL server,从中选择所需的服务器。

4. 请选择"Windows身份验证"或"SQL Server身份验证"。我们建议您选择后一个选项。

5. 输入SQL Server用户名和密码。

注意:选择的用户在SQL Server中应该被赋予sysadmin的角色。如果您使用本地系统管理员或域管理员来运行 Lepide数据安全平台服务,则其登录与Windows身份验证和sysAdmin角色应该存在于SQL Server中。

6. 单击Next继续。下步显示Database Settings。

数据库设置执行以下步骤配置数据库设置。

7. 输入SQL Server的名称。您也可以单击图标枚举所有SQL server列表,从中选择需要的SQL server。

8. 选择身份验证类型, 最好是SQL身份验证。

9. 输入SQL管理用户的登录凭据。

注意:此处选择的用户应该在SQL Server中具有dbcreator角色,审计数据必须存储在SQL Server中。

10. 输入存储审计日志的数据库名称。下面的屏幕截图显示了示例细节。

注意:单击该图标将在"默认SQL Server设置"中将当前SQL Server设置保存为默认设置。

11. 单击"测试连接",测试与SQLServer的连接。

			_		×
Database Sett	tings				
Please enter SQL s	erver details to store data	a			
Configure SQL Se	erver				_
SQL Server :	LDSP_SQL				
	Authentication Windows Authentic	ation			
	User Name :	sa			
	Password :	******	Test Connecti		
Select Database:	Lepide SQLDB		Test Commedia		·
			< <u>B</u> ack	Finish	Cancel

添加SQL Server高级配置

1. 在下面的向导中, 您需要选择"Advanced Configuration"选项。

			×
Configuration Type			
Please select configuration method.			
C Express Configuration			
(Configure the SQL Server with default settings)			
 Advanced Configuration 			
(Configure the SQL Server each settings individually)			
	< <u>B</u> ack	<u>N</u> ext >	Cancel

13. 单击Next。

SQL运行状况监视

14. 下一步显示SQL Server运行状况监视设置。

	igo	
ease enter nost creden	tials to monitor sqt. server health.	
Health Monitoring		
Enable Health Monit	oring	
Computer Name	LPSQLSRV	
1210723000	1	
User Name	lepide corporate administrator For Example : Domain\UserName	
Password	******	

- 15. 选中"启用运行状况监视"复选框以启用SQL Server的运行状况监视。您必须提供安装SQL Server的计算机的以下详细信息。
- a. "计算机名":输入安装SQL Server的计算机名称或IP地址。

b. 用户名:提供该计算机的管理员用户名(也可以是域管理员用户)。

c. 密码:输入上述用户的密码。

16. 单击Next继续。

下一步显示审计设置。

审计设置

Audit Settings			
Please select audit o	options to audit		
Auditing Type			
Select :	Audit Everything	-	

17. 在这里, 您需要指定审计类型。

a. 审计一切: SQL Server上的一切,包括所有服务器对象和数据库都将被审计。

b. 审计服务器:只审计服务器对象,不审计数据库。

c. 审计服务器与选定的数据库: 所有服务器对象和仅选中的数据库对象将被审计。如果选择此选项, 则必须选择 要审计的 数据库。

	Sele	Audit Server and selected databases objects
	10	Databases
-		Lepide FS DB
		Lepide SQLDB
		Lepide_AD_April
1		Lepide_Dropbox
		Lepide_SQLDB
		Lepide-AD-2022
		Lepide-AD-2022_1
		Lepide-Console
		Lepide-DDC-MasterCC
		Lepide-DDC-P
		Lepide-Fileserver
		Lepide-FS
-		LepideFSA DB
		LepideFSA DB_2022
		Lepide-Permissions
	H	Lepide-Permissions_DC5/
	H	Lepide Sult Tracker
L	P	tempab

18. 选中要审计的数据库的复选框。未选中的数据库将不会被审计或监视。单击"下一步"。下一步是"对象设置"。

对象设置

Please select objects(s) and operation(s) to be audited

Sel	lect	Ob	iects	to	Audit
			1		

Objects	Operations
Server Objects	
Login	Created;Dropped;Altered;Failed
 Alert 	Created;Dropped;Altered
DTS Package	Created;Dropped
Database	Created;Dropped;Altered
Database Backup	Created
Database Restore	Created
Job	Created;Dropped;Altered
Database Replication	Created;Dropped;Altered
Server Permissions	Altered
Database Objects	
Table	Created;Dropped;Altered
Stored Procedure	Created;Dropped;Altered
Trigger	Created;Dropped;Altered
Function	Created;Dropped;Altered
User	Created;Dropped;Altered
Role	Created;Dropped;Altered
Data Type	Created;Dropped;Altered
Default	Created;Dropped;Altered
Rule	Created;Dropped;Altered
View	Created;Dropped;Altered
Full Text Catalog	Created;Dropped;Altered
	C Bask Nava -

19. 在此步骤中,您可以指定要审计的服务器对象、数据库对象和操作。您可以选中需要监控的对象的复选框。此外,您可以单击对象的操作列表,以选择哪些操作必须包含在审计中或从审计中排除。按照以下步骤选择对象的操作。

•选择服务器或数据库对象的操作单元格。

✓ Server Objects		
Login	Created;Dropped;Altered;Failed	*

•它会显示箭头。单击向下箭头以访问操作列表。

Objects	Operations
Server Objects	
Login	Created;Dropped;Altered;Failed
 Alert 	
DTS Package	Created
Database	Dropped
Database Backup	Altered
Database Restore	Failed
Job	
Database Replication	
Server Permissions	
▲ Database Objects	
Table	
Stored Procedure	
Trigger	OK Cancel
Function	cioacoa, proppoa, acioa

•取消勾选不需要审计的操作。

Server Objects					
Login	Created;Dropped;Altered;Failed				
Alert					
DTS Package	Created				
Database	Dropped				
Database Backup	Altered				
Database Restore	Failed				
Job					
Database Replication					
Server Permissions					
Database Objects					
Table					
Stored Procedure					
Trigger	OK Cancel				
Function	areatos, aroppos, ritoros				

•单击"确定",修改Loginobject的操作选择。

✓ Server Objects		
Login	Created;Failed	.

•单击"下一步"。下一页显示UserSettings。

用户设置

				×
User Settings				
Please select SQL Se	erver user(s) to be audited			
Select Users to Au	dit			
Audit:	All Users	τi.		
Users				
				C 1
		 < <u>B</u> ack	Next >	Cancel

"用户设置"有以下选项。

- 审计所有用户: 审计所有用户。
- Audit Selected Users:选中该选项, 启用Users部分, 枚举所有SQL用户。

	Audit: Selected Users
	Users
	##MS_PolicyEventProcessingLogin##
	##MS_PolicyTsqlExecutionLogin##
	LDSP36DB\Administrator
	Lepide SQL
	LPDE3\Administrator
	LPDE3\sumit
	LSTAgentLogin
_	NT AUTHORITY\SYSTEM
	NT SERVICE\MSSQLSERVER
	NT SERVICE\SQLSERVERAGENT
	NT SERVICE\SQLTELEMETRY
_	NT SERVICE\SQLWitter
_	NI SERVICE\Winmgmt
_	sa sa

20. 在这里,您可以选中要审计的用户,取消选中以排除审计的其他用户。

21. 单击Next。下一页显示数据库设置。

存档数据库设置

22. 在此步骤中, 您需要提供存档数据的详细信息。这是一个可选步骤, 如果您不想归档审计数据, 可以跳过它。

					×
Archive Settings					
Please configure the s	ettings to archive the old logs				
<u> </u>					
Archive Audit Da	ta				
Configure SQL Serv	/er				
SQL Server :					
Au	uthentication				
	Windows Authentication				
	SQL Authentication				
	User Name :				
	Password :				
			T C	0	
			Test Connection		
Database Name :					
Schedule					
Waekly	Monthly				
A	Deve				
Archive Older than	Uays	<u> </u>			
Delete records fro	m current database after archiv	ing			
			< <u>B</u> ack	inish	Cancel

23. 归档数据库设置是在添加域的过程中讨论的。有关更多信息,请参阅我们的Active Directory高级配置指南。

24. 单击Finish完成该过程。

在执行了通过"快速配置"或"高级配置"添加SQL Server的所有步骤后,屏幕上将出现一个需要重新启动解决方案权限的消息框。



- 25. 单击Yes重新启动解决方案。
 - 15 haocst.com | 虹科的网络安全部

26. 重新启动后,将在Radar和Health Monitoring选项卡中创建一个新选项卡。一旦重新启动,在Radar选项卡下创建 一个新的SQL Server选项卡。

Jula Security Platform			
unit Georgiales kirghts - Silk Analysis - Silk Veis - File Server - Silk Server - Over	-		
erver : 192.168.10.29		View : Default	- A41 (F
			Information updated on : 01/25/2023 445:30
42			
Total changes made in SQL Server today			
LiveFeed			Creans Aint
Seath			P
-SQL Modification Feed- Alet Name : SQL29 Alerts			
01/25/2023 4:30:27 9M Table : Customer Data			
was Aftered by sa From DEWOSCL21F			
Aint Name SQL20 Aints			
Table : Customer_Data			
und de stadu el la segue provisione el			
-SQL Modification Feed-			
Hat Name (2013) Hatty			
Chariges by Criticality	2 0 0	Failed Logon Trend	0 0 0
Current and the control of the Contr		37	
High, 4	#.		
	N		
			Sector ate Windows
			Active Center to activate Wildows

• SQL Server管理允许您管理和删除SQL Server列表。在这里,您可以卸载审计代理、配置审计、重新安装审计代理和管理运行状况监视。



www.haocst.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

haocst.com