NO : Green Trend(GT2019-SEB507)







SQL专家云服务热线:4000-345-010 北原楷瑞趋势科技有限公司 | www.zhuancloud.com 东升科技园北领地D-3摄



安易备部署使用手册

© Copyright 北京格瑞趋势科技有限公司 Corporation 2019. All rights reserved.



第1章	环境准备	. 3
1.1	操作系统版本	. 3
1.2	数据库版本	. 3

1 格瑞捷	到外
1.3 🕅	络
1.4 生	产数据库服务器
1.4.1	.Net 版本
1.4.2	数据备份
1.5 数	据库帐号
第2章 安	装安易备软件
2.1 命	令一览
2.1.1	New-LocalInstance:添加本地实例
2.1.2	New-PrimaryInstance:添加主实例
2.1.3	New-Database:添加数据库
2.1.4	Remove-Database : 删除数据库
2.1.5	New-Licence:添加授权许可
2.1.6	Reset-LocalInstance:修改本地实例配置
2.1.7	Remove-PrimaryInstance : 删除主实例
2.1.8	Remove-LocalInstance : 删除本地实例
寛3章 配	置安易备
3.1 安	装代理服务
3.2 安	易备服务器端
3.3 添	加生产服务器
3.4 添	加数据库
3.5 修	改、删除安易备配置
	北京格瑞趋势科技有限公司: <u>www.grqsh.com</u> 热线电话:4000-345-010

格	瑞趋势
3.6	验证配置13
3.7	授权13
第4章	网络配置15
4.1	开启防火墙15
4.2	修改远程端口15
4.3	配置端口安全策略16
第5章	灾难恢复19
5.1	拷贝文件19
5.2	启用安易备服务器19

5

第1章 环境准备

1.1 操作系统版本

部署安易备备需要在以下操作系统环境中

Windows Server 2012\2012R2\2016 Standard/DataCenter 及以上

1.2 数据库版本

安易备是对生产服务器数据库备份进行安全备份的,所以装有安易备软件的服务器中也要安装

与生产服务器版本一致的数据库,目前安易备支持以下版本的数据库

SQL Server 2005 标准版/企业版

SQL Server 2008 标准版/企业版

SQL Server 2008 R2 标准版/企业版

SQL Server 2012 标准版/企业版

SQL Server 2014 标准版/企业版

SQL Server 2016 标准版/企业版

SQL Server 2017 标准版/企业版

1.3 网络

与生产服务器网络互通,端口互通

1.4 生产数据库服务器

1.4.1.Net 版本

生产服务器如果是 Windows Server 2008 R2 以前的版本,需要安装.net4.0 版本以上框架

1.4.2 **数据备份**

需要进行安易备安全备份的数据库需要加入到定期执行备份的计划任务中

1.5 数据库帐号

需要在生产服务器和安易备数据库上各创建一个 safe_backup_user 帐号, 权限为 sysadmin, 密码

保持一致。

第2章 安装安易备软件

2.1 命令一览

2.1.1 New-LocalInstance: 添加本地实例

名称	作用	必须	默认值
LocalInstance	本地实例的实例名,通过该实例名要能	是	
	够连接到本地实例		
LocalBackupDirectory	本地实例的备份文件路径	是	
LocalDataDirectory	本地实例下的还原数据库数据文件的	是	
	路径		
LocalLogDirectory	本地实例下的还原数据库日志文件的	否	参数
	路径		LocalDataDirectory 的
			值
AgentPort	代理服务通讯端口	否	0
CopyFrequency	拷贝备份文件任务的频率,单位:秒	否	10
RestoreFrequency	还原备份文件任务的频率,单位:秒	否	10
CleanFrequency	清理过期备份文件任务的频率,单位:	否	60
	秒		
Timeout	超时时间,单位:秒	否	30

2.1.2 New-PrimaryInstance: 添加主实例

名称	作用	必	默认值
		须	
LocalInstance	本地实例的实例名,通过该实例	是	
	名要能够连接到本地实例		
PrimaryInstance	主实例的实例名,通过该实例名	是	
	要能够连接到主实例		
UserName	连接主实例使用的登录账户	是	
PrimaryBackupDirectory	主实例下的备份文件的路径	是	只有此目录下的备份文件
			才会同步
PrimaryBackupNetworkDirectory	主实例下的备份文件的网络路	否	默认空值,如果要使用共
	径		享目录, 需要设置为参数
			PrimaryBackupDirectory
			的值
Timeout	超时时间,单位:秒	否	30

2.1.3 New-Database:添加数据库

名称	作用	必	默认值
		须	
LocalInstance	本地实例的实例名,通过该实例	是	
	名要能够连接到本地实例		
PrimaryInstance	主实例的实例名,通过该实例名	是	
	要能够连接到主实例		
PrimaryDatabaseName	主实例下数据库的名称	是	
LocalDatabaseName	本地实例下数据库的名称	否	参数
			PrimaryDatabaseName
			的值
PrimaryBackupDirectory	该数据在主实例下的备份文件的	否	实例同参数的值
	路径		
PrimaryBackupNetworkDirectory	该数据在主实例下的备份文件的	否	实例同参数的值
	网络路径		
LocalBackupDirectory	该数据库在本地实例下的备份文	否	实例同参数的值
	件的路径		
LocalDataDirectory	该数据库在本地实例下数据文件	否	实例同参数的值
	的路径		
LocalLogDirectory	该数据库在本地实例下日志文件	否	参数
	的路径		LocalDataDirectory 的
			值
FileRetentionPeriod	在本地实例中保留该数据库备份	否	15
	文件的天数		
Timeout	超时时间,单位:秒	否	30

2.1.4 Remove-Database: 删除数据库

名称	作用	必须	默认值
LocalInstance	本地实例的实例名,通过该实例名要能够	是	
	连接到本地实例		
LocalDatabaseName	本地实例下数据库的名称	是	
RetainDatabase	是否在本地实例中保留数据库,0:不保留;	否	0
	1: 保留		
RetainBackupFile	是否在本地实例中保留备份文件, 0: 不保	否	0
	留; 1: 保留		
DeletePrimaryLog	是否删除主实例下的日志数据,0:不删除;	否	1
	1: 删除		
Timeout	超时时间,单位:秒	否	30

名称	作用	必须	默认值
LocalInstance	本地实例的实例名,通过该实例名要能够连	是	
	接到本地实例		
PrimaryInstance	使用该授权码的主实例名,要要授权码里面	是	
	的一致		
Licence	授权码	是	
Timeout	超时时间,单位:秒	否	30

2.1.5 New-Licence:添加授权许可

2.1.6 Reset-LocalInstance:修改本地实例配置

名称	作用	必须	默认值
LocalInstance	本地实例的实例名,通过该实例名要能	是	
	够连接到本地实例		
LocalBackupDirectory	本地实例的备份文件路径	否	
LocalDataDirectory	本地实例下的还原数据库数据文件的	否	
	路径		
LocalLogDirectory	本地实例下的还原数据库日志文件的	否	
	路径		
AgentPort	代理服务通讯端口	否	
CopyFrequency	拷贝备份文件任务的频率,单位:秒	否	
RestoreFrequency	还原备份文件任务的频率,单位:秒	否	
CleanFrequency	清理过期备份文件任务的频率,单位:	否	
	秒		
Timeout	超时时间,单位:秒	否	30

2.1.7 Remove-PrimaryInstance:删除主实例

名称	作用	必	默认值
		须	
LocalInstance	本地实例的实例名,通过该实例	是	
	名要能够连接到本地实例		
PrimaryInstance	主实例的实例名,通过该实例名	是	
	要能够连接到主实例		
Timeout	超时时间,单位:秒	否	30

2.1.8 Remove-LocalInstance: 删除本地实例

名称	作用	必须	默认值		
LocalInstance	本地实例的实例名,通过该实例名要能够	是			
北京格瑞趋势科技有限公司: <u>www.grqsh.com</u> 热线电话:4000-345-010					
7 / 21					

🔒 格瑞趋势

勒索病毒的最后一道防线

	连接到本地实例		
RetainBackupFile	是否在本地实例中保留备份文件, 0: 不保	否	0
	留; 1: 保留		
Timeout	超时时间,单位:秒	否	30

北京格瑞趋势科技有限公司:<u>www.grqsh.com</u>热线电话:4000-345-010

8 / 21

🚯 格瑞趋势

第3章 配置安易备

3.1 安装代理服务

首先需要在生产服务器上安装安易备软件的代理服务,通过代理服务将生产数据库的备份文件 拉取到安装了安易备软件的服务器中。

将代理服务文件夹拷贝到生产服务器中,不要放在 C 盘,

E	agent_service		2019/8/2 11:05	文件夹	
	backup		2019/8/2 11:17	文件夹	
	sxs		2019/8/2 10:48	文件夹	
0	cn_sql_server_2014	_enterprise_editio	2018/6/22 16:30	光盘映像文件	3,436,520

打开文件夹选择'安装安易备代理服务_Install'文件,运行安装

📧 GreenTrend.SafeBackup.Agent.Service	2019/8/1 14:48	应用程序	14 KB
📑 GreenTrend.SafeBackup.Agent.Servic	2019/7/22 10:34	XML Configurati	1 KB
📄 GreenTrend.SafeBackup.Agent.Servic	2019/8/2 11:05	INSTALLLOG 文件	1 KB
📄 GreenTrend.SafeBackup.Agent.Servic	2019/8/2 11:05	INSTALLSTATE	8 KB
📄 GreenTrend.SafeBackup.Agent.Servic	2019/8/1 14:48	PDB 文件	30 KB
InstallUtil.InstallLog	2019/8/2 11:05	INSTALLLOG 文件	1 KB
◎ 安装安易备代理服务_Install	2019/6/27 17:19	Windows 批处理	1 KB
💿 卸载安易备代理服务_UnInstall	2019/6/27 17:20	Windows 批处理	1 KB

安装成功后,可以打开 windows 服务看到已安装好的安易备代理服务

👔 格瑞趋势

勒索病毒的最后一道防线

🔍 服务			_		×
文件(F) 操作(A) 3	查看(V) 帮助(H)				
() 🗐 📊 ()) 🔂 🚺 🖬 🕨 🔲 II 🕪				
🔍 服务(本地)	① 服务(本地)				
	GreenTrend SafeBackup Agent	~	描述	状态	^
	Service	🎑 Geolocation Service	此服务将监视系统的…	正在运行	ř 🛛
	体。同时网友	🧠 GreenTrend SafeBackup Agent Servi	安易备代理服务,如…	正在运行	
	<u>停止</u> 吃服务 重启动比服务	🤹 Group Policy Client	此服务负责应用管理…	正在运行	ř –
		🎑 Human Interface Device Service	激活键盘、遥控器和…		
		🔍 HV 主机服务	为 Hyper-V 虚拟机监		
	GreenTrend SafeBackup Agent Service 名称 停止此服务 重启动此服务 Geolocation Service 停止此服务 GreenTrend SafeBack 通知此服务 Group Policy Client 通知比服务 Human Interface Det 日本 描述: 安易备代理服务,如果停止服务将无 法同步备份文件。 Hyper-V Data Excha Gener-V Data Excha Gener-V Data Excha Gener-V Data Excha Gener-V PowerShell Gener-V PowerShell Gener-V Time Synch	🎑 Hyper-V Data Exchange Service	提供一种机制,用于…		
	安易番代理服务,如果停止服务将无 注同先条公文件	🎑 Hyper-V Guest Service Interface	为 Hyper-V 主机提供		
		🎑 Hyper-V Guest Shutdown Service	提供一种机制,用于…		
		🎑 Hyper-V Heartbeat Service	通过定期报告检测信…		
		🍓 Hyper-V PowerShell Direct Service	提供了一种在不使用		
		🍓 Hyper-V Time Synchronization Service	将此虚拟机的系统时…		
		🎑 Hyper-V 卷影复制请求程序	协调使用卷影复制服…		
		🔍 Hyper-V 远程桌面虚拟化服务	提供一个平台以在虚…		
		🖳 IKE and AuthIP IPsec Keying Modules	IKEEXT 服务托管 Int	正在运行	ŕ

3.2 安易备服务器端

1. 加载安易备模块

在 powershell 里执行 cd c:\safe_backup 进入文件夹(safe_backup 文件夹在那个盘符前面就写 哪个盘符),接着输入.\bin\install.ps1 按回车

PS C:\Users\Administrator> cd d:\safe_backup PS D:\safe_backup> .\bin\Install.ps1

 创建数据库,作业,拷贝路径,端口,还原路径 在安易备创建 safe_backup_master 数据库,作业,与生产端安装的代理服务相对应的端口, 以及拷贝文件的路径和数据库还原路径:

New-LocalInstance -LocalInstance "<mark>输入安易备数据库服务器 IP 或数据库实例名</mark>" -AgentPort "8253" -LocalBackupDirectory "<mark>安易备存放拷贝回来备份文件的路径</mark>" -LocalDataDirectory "

安易备在本地还原校验备份文件的路径"

示例:

在安易备服务器上打开 PowerShell 命令执行窗口,执行脚本命令

PS C:\Usere\Administrator> New-LocalInstance -LocalInstance "192.163.1.189" -AgentPort "8253" -LocalBackupDirectory "d:\backup_dir" -LocalDataDirectory "d:\backup_data" 创建 safe backup_master 数据库 保存本地交例配置 创建本地数据文件目录 创建本地数据文件目录 创建 : 恢复、作业 创建 : 清理、作业 创建 : 清理、作业 成功

北京格瑞趋势科技有限公司:<u>www.grqsh.com</u>

3.3 添加生产服务器

命令执行成功后会在生产端服务器上创建 safe_backup_log 数据库,该数据库记录了安易备操作日志:

New-PrimaryInstance -LocalInstance "輸入安易备数据库服务器 IP 或数据库实例名" -PrimaryInstance "輸入生产服务器 IP 或数据库实例名" -UserName "safe_backup_user"-PrimaryBackupDirectory "生产 服务器存放备份文件的路径"

示例:

在安易备服务器上打开 PowerShell 命令执行窗口,执行脚本命令

本地实例的连接 数据有效性 王买例的连接 ·safe_backup_log'数据库 主实例

3.4 添加数据库

将生产服务器数据库添加到安易备服务器中,命令每次执行只能添加一个数据库,如有多个数

据库,需要多次执行脚本命令。

New-Database -LocalInstance "输入安易备数据库服务器 IP 或数据库实例名" -PrimaryInstance "输入 生产服务器 IP 或数据库实例名" -PrimaryDatabaseName "生产服务器数据库名称"

示例:

在安易备服务器上打开 PowerShell 命令执行窗口,执行脚本命令



3.5 修改、删除安易备配置

▶ 修改本地实例配置(LocalInstance 必选,其它参数可选):

	格瑞 趋势 教家病毒的最后一道防线
7	在安易备服务器上打开 PowerShell 命令执行窗口,执行脚本命令
	Reset-LocalInstance -LocalInstance " <mark>输入安易备数据库服务器 IP 或数据库实例名</mark> "-
	LocalBack1upDirectory " <mark>安易备存放拷贝回来备份文件的路径</mark> " -LocalDataDirectory " <mark>安易备在本</mark>
	<mark>地还原校验备份文件的路径</mark> " -AgentPort "8000" -CopyFrequency "30" -RestoreFrequency "30" -
	CleanFrequency "60"

▶ 删除数据库:

在安易备服务器上打开 PowerShell 命令执行窗口,执行脚本命令

Remove-Database -LocalInstance "输入安易备数据库服务器 IP 或数据库实例名" -

LocalDatabaseName "加入到安易备的生产数据库名称"

> 删除主实例:

在安易备服务器上打开 PowerShell 命令执行窗口,执行脚本命令

Remove-PrimaryInstance -LocalInstance "输入安易备数据库服务器 IP 或数据库实例名" -

PrimaryInstance "输入生成服务器 IP 或数据库实例名"

> 删除本地实例(不保留备份文件):

在安易备服务器上打开 PowerShell 命令执行窗口,执行脚本命令

Remove-LocalInstance -LocalInstance "输入安易备数据库服务器 IP 或数据库实例名"

▶ 删除本地实例(保留备份文件):

在安易备服务器上打开 PowerShell 命令执行窗口,执行脚本命令

Remove-LocalInstance -LocalInstance "输入安易备数据库服务器 IP 或数据库实例名" -

RetainBackupFile "1"

卸载加载模块:

北京格瑞趋势科技有限公司:<u>www.grqsh.com</u>

<u>n</u> 热线电话:4000-345-010

 $12 \ / \ 21$

👔 格瑞趋势

勒索病毒的最后一道防线

在安易备服务器上打开 PowerShell 命令执行窗口,执行脚本命令

cd c:\safe_backup

.\bin\UnInstall.ps1

3.6 验证配置

1) 在生产服务器上,从日志库 safe_backup_log,查询安易备运行情况情况,如下图,可以看到拷贝还 原是否成功 (select * from 表名 order by id desc)

SQLQuery2.sql - 192.168.1.138.safe_backup_mas	ster (sa	(59))* - Microsoft SQL Se	rver Managen	nent Studio								- 0 ×
文件(F) 编辑(E) 视图(V) 查询(Q) 项目(P) 调试	(D) I	[具(T) 窗口(W) 帮助(H)										
🔄 • 💷 - 🥁 🛃 🐊 🔔 新建查询(N) 📑 🔧 🕤	6 6	🔏 🕰 🔁 🔹 - (°' -	💭 - 🖾 🖂	×		- M	- 🖓 🕾 🌶	ê 💽 - 📮				
: 🖅 🔐 😽 safe_backup_master 🔹 📍 执行(X)	▶调	list(D) = 🗸 🚏 🗐 📃	17 4 0	💭 🕐 🖄 🖄 🐺	🗰 🖓 🖕							
対象资源管理器 ▼ 早 ×	SQLC	Query2.sql - 1master (s	a (59))* 🗙 S0	QLQuery1.sql - 1ma	ster (sa (56))*					-	尾性	- 4 ×
连接• 對 對 = 7 🗑 🔏		select * from [dbo]	[tb1_sb_cop	oy_log] order by i	d desc					÷	当前连接参数	
□ P 192 168 1 145 (SQL Server 12.0 5000.0 - sa)										~	23 61 103	
□ □ 数据库											 ▼ 服合状态 	
🗄 🗀 系统数据库						本 海 洒 石					版回的行数	1256
🗉 🗀 数据库快照						<>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>					结束时间	2018/12/25 17:02:22
⊟ isafe_backup_log											开始时间	2018/12/25 17:02:22
🗄 🗀 数据库关系图											连接失败	
🛛 🗀 表											名称	192.168.1.138
🗄 🗀 系统表	LE RA	D ±									占用时间	00:00:00.367
FileTables	同际	口心									状态	打开
dbo.tbl_sb_clean_log											✓ 连接	
dbo.tbl_sb_copy_log	拷贝	日志									连接名称	192.168.1.138 (sa)
III III IIII III III IIII III IIII II						IF <i>h</i>	4.4.古时间				➤ 连接详细信息	
						713	USD WEITING	*	犬态		SPID	59
	▲ 还师	原日志							1		登录名	sa
III 🗀 Service Broker									1		返回的连接行数	1256
🗉 🗀 存储										× 1	服务器版本	12.0.5000
🗉 🗀 安全性	100 %									- 1	服务器名称	192.168.1.138
🗄 📒 xiao	- -	3果 🛅 消息									会活跟踪 ID	
🗄 🔰 xiaohao		kup_finish_date	backup_size	first_lsn	last_lsn	start_time	finish_time	duration	a nessage	^	连接结束时间	2018/12/25 17:02:22
■ 📮 安全性	1	8-12-25 17:02:18.000	77824	19900000030000001	19900000034400001	2018-12-25 17:02:21.277	2018-12-25 17:02:21.453	0	success	- 1	连接升如时间	2018/12/25 17:02:22
□ □ 版务器対象	2	8-12-25 17:02:05.000	407552	19900000032800034	19900000034400001	2018-12-25 17:02:04.143	2018-12-25 17:02:04.317	0	success		连接占用时间	00:00:00.367
	3	8-12-25 17:02:04.000	2897920	19900000030400034	19900000032000001	2018-12-25 17:02:03.437	2018-12-25 17:02:04.120	1	success		连接状态	打开
Alwayson multit	4	8-12-25 17:02:04.000	77824	19900000029600001	19900000030000001	2018-12-25 17:02:02.467	2018-12-25 17:02:03.390	1	success		显示名称	192.168.1.138
Integration Services 日录	5	8-12-25 17:01:47.000	77824	19900000029300001	19900000029600001	2018-12-25 17:01:51.517	2018-12-25 17:01:51.757	0	success		1	
I B SOL Server 代理	6	8-12-25 17:01:34.000	407552	19900000029000001	19900000029500001	2018-12-25 17:01:34.050	2018-12-25 17:01:34.170	0	success		1	
	7	8-12-25 17:01:34.000	77824	19900000026400001	19900000029300001	2018-12-25 17:01:31.680	2018-12-25 17:01:34.043	3	success		1	
	8	8-12-25 17:01:09.000	407552	19900000027400034	19900000029000001	2018-12-25 17:01:21.427	2018-12-25 17:01:21.690	0	success		1	
	9	8-12-25 17:01:08.000	2897920	19900000024700037	19900000026600001	2018-12-25 17:01:07.660	2018-12-25 17:01:11.153	4	success		1	
	10	8-12-25 17:01:04.000	77824	19900000024200001	19900000026400001	2018-12-25 17:01:04.620	2018-12-25 17:01:07.413	3	success		1	
	11	8-12-25 17:00:47.000	77824	19900000023900001	19900000024200001	2018-12-25 17:00:51.267	2018-12-25 17:00:51.510	0	success		1	
	12	8-12-25 17:00:36.000	407552	19900000023600001	19900000024100001	2018-12-25 17:00:41.753	2018-12-25 17:00:43.193	2	success		1	
	13	8-12-25 17:00:36.000	77824	19900000021000001	19900000023900001	2018-12-25 17:00:41.250	2018-12-25 17:00:41.710	0	success	~		
	<								>		名称	
	2 査	向已成功执行。				192.168.1.138 (12.0 SP2)	sa (59) safe_backup_mast	er 00:00:	00 1256	īΞ	建接的名称。	
就站								行	1	列:	55 字符55	5 Ins

3.7 授权

添加授权:

New-Licence -LocalInstance "輸入安易备数据库服务器 IP 或数据库实例名" -PrimaryInstance "输入生 产服务器 IP 或数据库实例名" -Licence "授权码"

参数属性:

-LocalInstance ""(本地安易备的 IP)

-PrimaryInstance ""(生产端服务器 IP)

北京格瑞趋势科技有限公司:<u>www.grqsh.com</u>

13 / 21

能瑞趋势

勒索病毒的最后一道防线

查看授权:

Get-Licence -LocalInstance "输入安易备数据库服务器 IP 或数据库实例名"

参数属性:

-LocalInstance ""(本地安易备的 IP)

查看安易备版本号:

Get-About

🏦 格瑞趋势

勒索病毒的最后一道防线

第4章 网络配置

4.1 开启防火墙

防止外部网络访问

🔐 本地计算机 上的高级安全 Wind	本地计算机 上的高级安全 Windows 防火墙
🧱 入站规则 🌠 出站规则 毳 连接安全规则	A 高级安全 Windows 防火墙为 Windows 计算机提供网络安全。
> 🌉 监视	概述 域配置文件是活动的 ② Windows 防火墙已启用。 ③ 阻止与规则不匹酉的入站连接。 ④ 位に生物则不匹酉的入站连接。
	 ♥ パド与规则不匹置的出始连接。 ● 毎月配置文件 ● Windows 防火墙已启用。 ● 阻止与规则不匹置的入站连接。 ● 允许与规则不匹置的出站连接。
	 公用配置文件 Windows 防火墙已启用。 Mindows 防火墙高台 が許与規则不匹配的出站连接。 Windows 防火墙属性

4.2 修改远程端口

修改远程桌面端口为 33798, 重启操作系统生效

CMD 下执行

 $reg \ add \ "HKLM \ SYSTEM \ current Control Set \ Control \ Server \ Wds \ rdpwd \ Tds \ tcp'' \ /v$

PortNumber /t reg_dword /d 33798 /f

 $reg \ add \ "HKLM \ SYSTEM \ Current Control \ Set \ Control \ Terminal \ Server \ WinStations \ RDP-Tcp'' \ /v$

PortNumber /t reg_dword /d 33798 /f

修改远程默认端口后,在防火墙添加一条新远程端口的默认规则,

北京格瑞趋势科技有限公司: <u>www.grqsh.com</u> 热线电话: 4000-345-010

15 / 21

🚯 格瑞趋势

勒索病毒的最后一道防线

📸 高级安全 Windows 防火墙	_ _ _ _ _ _ _ _ _ _ _
文件 (F) 操作 (A) 查看 (V) 帮助 (H)	
🔐 本地计算机 上的高级安全 Wire 入 <u>引把贝</u>	操作
	入站规则
	新建物则
	▼ 按配面又任师选 ►
「	▼ 按状态筛选
bùtan端口 bhùtan端口 bhùtanh bh	▼ 按组筛选 ▶
▲ 小议类型(P): TCP nchCache - 托管缓存 所	查看 ▶
	🖸 刷新
	📑 导出列表
	👔 帮助
□ 示例: 80、443、5000-5010 管理 所i	远程端口 🔺
	◆ 禁用规则
■ 〒例:80、443、5000-5010 SI服务 所:	🤞 剪切
	国新 夏制
Internet 控制消息协议 (CCMP) 设 要: 	
P Trap iš	□ 周性
P Trap 5	12 帮助

4.3 配置端口安全策略

在 CMD 窗口执行以下命令

rem #***************删除原有策略************************************
netsh ipsec static ^
delete policy name= GRQSHIpsec
rem ************创建安全策略************************************
netsh ipsec static ^
add policy name=GRQSHIpsec
rem #*************添加 2 个动作:允许和禁止************************************
netsh ipsec static ^
add filteraction name=允许 action=permit
netsh ipsec static ^
add filteraction name=禁止 action=block
rem #***************创建筛选器及列表************************************
netsh ipsec static ^
add filterlist name=port
北京格瑞趋势科技有限公司: <u>www.grqsh.com</u> 热线电话:4000-345-010
16 / 21

😭 格瑞趋势

勒索病毒的最后一道防线

```
netsh ipsec static ^
   add filter filterlist=port srcaddr=Any dstaddr=Me dstport=139 protocol=TCP
   netsh ipsec static ^
   add filter filterlist=port srcaddr=Any dstaddr=Me dstport=445 protocol=TCP
   netsh ipsec static ^
   add filter filterlist=port srcaddr=Any dstaddr=Me dstport=137 protocol=UDP
   netsh ipsec static ^
   add filter filterlist=port srcaddr=Any dstaddr=Me dstport=138 protocol=UDP
   netsh ipsec static ^
   add filter filterlist=port srcaddr=Any dstaddr=Me dstport=135 protocol=TCP
    netsh ipsec static ^
    add filter filterlist=port srcaddr=Any dstaddr=Me dstport=3389 protocol=TCP
    netsh ipsec static ^
   add rule name=port policy=GRQSHIpsec filterlist=port filteraction=禁止
   netsh ipsec static ^
   set policy name = GRQSHIpsec assign = y
@pause
```

🔒 格瑞趋势

🖥 本地安全策略					ſ
文件()》 操作(A) 查看(V) 帮助(H)					l
🗢 🔿 🙋 📅 🗟 🔒 🚺 🏦					
🚡 安全设置	名称 🔺	描述	策略已指	⑥ 上次更改时间	1
🗉 📴 帐户策略	🛃 GRQSHIpsec		是	2020/9/3 18:	ł
					I
Ⅰ ■ 高級安全 Windows 防火庫					I
■ 內疳刈液自理器束嗬 ■ ■ 外钼等略					I
□					I
Ⅲ 🧰 应用程序控制策略					I
🛃 IP 安全策略,在本地计算机					F
🗉 🧰 高级审核策略配置					I
					I
					l
					L
					L
					L
					L

北京格瑞趋势科技有限公司:<u>www.grqsh.com</u>

18 / 21

👔 格瑞趋势

第5章 灾难恢复

当生产服务器发生灾难性故障时, 安易备提供两种方式恢复数据供生产使用

5.1 拷贝文件

安易备是通过拉取生产服务器数据库备份文件的方式进行工作,因此安易备服务器上也存有一份生产数据库的备份文件,当生产服务器故障后,可以拷贝出这些备份文件,到临时生产服务器进行还原,恢复业务使用。

5.2 启用安易备服务器

安易备会把从生产服务器数据库拉取的备份文件进行自动还原校验,因此安易备上也会有根据 备份文件还原恢复的数据库存在,当生产服务器故障后,如果安易备服务器硬件配置可以临时支撑 起生产业务运行,也可以将安易备服务器充当生产服务器使用,由于安易备正常情况下是不支持访 问的,因此需要做以下几个操作才能将安易备服务器启用起来:

1. 添加规则

在防火墙添加一条允许访问端口为 1433 的入站规则

出站规则	1	к		组	^		配置文件	已启用	
	0	1433					所有	是	
ay 注按女王规则 ● № 监视		1433 属性				×	所有 所有	是 是	
	0	作用域	高级	本地主体	远程用户		所有	是	
	0	常规	程序和服务	远程计算机	协议和端口		所有	是	
	Ø	执动和端口					所有	是	
	0		ale Tril (=)				所有	是	
	0	🚽 🐨 ሙኑ	(奕型(ピ):	TCP	~		所有	是	
	0	10 W	(5(0):	6 🚽			公用	是	
	0	***	端出口(1.)・	特会進口	~		公用	是	
	0	~+~>0	, (L) H (L) .	1433			专用, 公用	是	
	0		L	7400 元前、00, 443, 5000-	0100		专用, 公用	是	
	0	远程	2 3 3 3 3 3 3 3 3 3 3 3 3 3 3 3 3 3 3 3	所有端口	~		公用	是	
							专用	문	

2. 安易备上的数据库是不支持正常写入的,需要执行以下 SQL 命令恢复正常。

RESTORE DATABASE DBName WITH RECOVERY

GO

3. 修改安易备 IP 为生产服务器 IP