Windows Server 操作系统
安全配置规范

龙岗区大数据管理局

2019 年 1 月 21 日

制作人	谢志超、潘一乐、温福城
审核人	张韶君
版本编号	SEC-2019-WINSERVER-V1

安全配置要求

1.1 账户失败次数锁定策略

项目编号	SEC-2019-WINSERVER-01-01-v1
配置说明	应配置账户失败次数锁定策略
配置指南	**1、参考配置** 打开命令提示符，运行命令“secpol.msc”打开本地安全策略，游览路径“安全设置\账户策略\账户锁定策略”，点击账户锁定策略，对其锁定策略设置如下规则： a.账户锁定时间（15 分钟）； b.账户锁定阈值（5 次无效登录）； c.重置账户锁定计数器（15 分钟）； **2、补充说明**
检测方法及判定依据	在一定时间内，连续使用错误密码达到设定阈值之后，锁定该账户预设时长，并在该时长之后自动解除
回退措施	取消账户锁定策略
备注	

1.2 密码策略

项目编号	SEC-2019-WINSERVER-01-02-v1
配置说明	应设置密码安全策略
配置指南	**1、参考配置**

	打开命令提示符，运行命令“secpol.msc”打开本地安全策略，游览路径“安全设置\账户策略\密码策略”，点击密码策略，对其密码策略设置如下规则： a.密码必须符合复杂性要求（已启用）； b.密码长度最小值（8个字符）； c.密码最短使用期限（2天）； d.密码最长使用期限（180天内）； e.强制密码历史（24个记住的密码）； f.用可还原的加密来存储密码（已禁用）； **2、补充说明**
检测方法及判定依据	重设的密码被强制满足复杂度要求，长度满足8个字符，且再次修改密码最短时间不低于2天。
回退措施	取消密码策略
备注	

1.3 审核策略

项目编号	SEC-2019-WINSERVER-01-03-v1
配置说明	应设置审核配置
配置指南	**1、参考配置** 打开命令提示符，运行命令“secpol.msc”打开本地安全策略，游览路径“安全设置\本地策略\审核策略”，点击审核策略，对所有的审核策略都开启成功、失败审核。

	2、补充说明
检测方法及判定依据	打开事件查看器，查看是否有日志生成
回退措施	取消对应审核策略
备注	

1.4 应用程序日志文件策略

项目编号	SEC-2019-WINSERVER-01-04-v1
配置说明	设置应用程序日志文件达到最大大小时的动作的序号
配置指南	**1、参考配置** 打开命令提示符，运行命令“eventvwr.msc”打开事件查看器，浏览到路径“事件查看器(\Windows 日志)\应用程序(日志)”，右键点击“应用程序(日志)”，打开其属性对话框，切换到“常规”选项卡，配置“日志文件达到最大大小时”为“按需要改写(覆盖)事件”以及配置日志最大大小为 81920KB。注意：对于其他项的安全（日志）、setup(日志)、系统（日志）也按照应用程序（日志）配置。 **2、补充说明**
检测方法及判定依据	日志大小能达到最大设置值，且覆盖动作按照预设值值进行。
回退措施	

备注	

1.5 连接超时策略

项目编号	SEC-2019-WINSERVER-01-05-v1
配置说明	应配置暂停会话前所需要的空闲时间数量
配置指南	**1、参考配置** 打开命令提示符，运行命令“secpol.msc”打开本地安全策略，游览路径“安全设置\本地策略\安全选项”，点击安全选项，找到“Microsoft 网络服务器：暂停会话前所需要的空闲时间数量”，双击选择“本地安全设置”，选择“中断连接如果空闲时间超过”，配置其内容为 15 分钟。 **2、补充说明**
检测方法及判定依据	
回退措施	
备注	

1.6 登录超时自动注销用户

项目编号	SEC-2019-WINSERVER-01-06-v1
配置说明	应配置登录时间用完时自动注销用户
配置指南	**1、参考配置**

	打开命令提示符，运行命令“gpedit.msc”打开组策略编辑器，浏览到路径“本地计算机策略\计算机配置\Windows 设置\安全设置\本地策略\安全选项”，在右边窗格中找到“(Microsoft 网络服务器：）当登录时间用完时自动注销用户”(适用于 Windows2000、WindowsXP、Windows2003、Windows2003R2)或“Microsoft 网络服务器：登录时间过期后断开与客户端的连接”，配置为“已启用”。 **2、补充说明**
检测方法及判定依据	
回退措施	
备注	

1.7 重命名管理员账户名

项目编号	SEC-2019-WINSERVER-01-07-v1
配置说明	应修改默认管理用户名
配置指南	**1、参考配置** 打开命令提示符，运行命令“gpedit.msc”打开组策略编辑器，浏览到路径“本地计算机策略\计算机配置\Windows 设置\安全设置\本地策略\安全选项”，在右边窗格中找到“(帐户:)重命名(系统)管理员帐户”，更改其默认管理用户名

	（默认为“Administrator”，更改成其他字段）。 **2、补充说明**
检测方法及判定依据	
回退措施	
备注	

1.8 禁用 Guest 账户

项目编号	SEC-2019-WINSERVER-01-08-v1
配置说明	应禁用 Guest 账户
配置指南	**1、参考配置** 打开命令提示符，运行命令“gpedit.msc”打开组策略编辑器，浏览到路径“本地计算机策略\计算机配置\Windows 设置\安全设置\本地策略\安全选项”，在右边窗格中找到“(帐户:)来宾帐户状态”，配置为“已禁用”。 **2、补充说明**
检测方法及判定依据	
回退措施	
备注	

1.9 禁用可匿名访问的共享

项目编号	SEC-2019-WINSERVER-01-09-v1
配置说明	应禁用可匿名访问的共享
配置指南	**1、参考配置** 打开命令提示符，运行命令“gpedit.msc”打开组策略编辑器，浏览到路径“本地计算机策略\计算机配置\Windows 设置\安全设置\本地策略\安全选项”，在右边窗格中找到“网络访问：可匿名访问的共享”，配置为空。 **2、补充说明** 此项不适用于域控服务器。
检测方法及判定依据	
回退措施	
备注	

1.10 禁用 Windows 硬盘默认共享

项目编号	SEC-2019-WINSERVER-01-10-v1
配置说明	设置是否禁用 Windows 硬盘默认共享
配置指南	**1、参考配置** 打开命令提示符，运行命令“compmgmt.msc”打开计算机管理面板，浏览到路径“计算机管理(本地)\系统工具\共享文件夹\共享”，删除所有硬盘默认共享；然后，在命令提示符中运行命令“regedit”打

	开注册表编辑器，浏览到路径“HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\LanmanServer\Parameters\”，添加名称为“AutoShareServer”和“AutoShareWks”、类型为 DWORD、数据为 0 的两个数值，若已存在则修改其数据。注意：若关闭 C 盘默认共享(C$)，将不能使用 BVS 的 SMB 扫描。 **2、补充说明** 此项仅适用于非域环境。
检测方法及判定依据	
回退措施	
备注	

1.11 开启系统防火墙

项目编号	SEC-2019-WINSERVER-01-11-v1
配置说明	设置开启系统防火墙
配置指南	**1、参考配置** 打开控制面板，选择 Windows 防火墙，点击“打开或关闭 Windows 防火墙”，选择启用 Windows 防火墙。 **2、补充说明** 在开启系统防火墙之前，先将必要的业务端口加入入栈请求允许访问。

检测方法及判定依据	
回退措施	
备注	

1.12 设置“锁定会话时显示用户信息”级别

项目编号	SEC-2019-WINSERVER-01-10-v1
配置说明	设置“锁定会话时显示用户信息”级别，建议设置为 3，不显示用户信息
配置指南	**1、参考配置** 打开命令提示符，运行命令“regedit”打开注册表编辑器，浏览到路径“HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System”，添加名称为“DontDisplayLockedUserId”、类型为 DWORD、数据为标准值的数值，若已存在则修改其数据。此数据的有效值为 1-3，其中 1 表示显示名称、域名、用户名，2 表示仅显示用户名称，3 表示不显示用户信息。WindowsXP 需要安装 207399 补丁才能生效；Windows2000 没有此设置，不检查此项。 **2、补充说明**
检测方法及判定依据	

回退措施	
備注	