**Windows server 2012 R2 安全加固**

|  |  |
| --- | --- |
| 基线项名称 | 设置密码使用期限策略 |
| 检查步骤 | 在管理工具打开本地安全策略，依次打开：安全设置—帐户策略—密码策略，检查密码最长使用期限与密码最短使用期限两项设置 |
| 基线合规性判定 | 密码最长使用期限设置为30-180之间，密码最短使用期限设置为1-14之间即合规，否则不合规 |
| 加固步骤 | 在管理工具打开本地安全策略，依次打开：安全设置—帐户策略—密码策略  检查密码最长使用期限与密码最短使用期限两项设置，将密码最长使用期限设置为30-180之间，建议值为90；  将密码最短使用期限设置为1-14之间，建议值为7。 |

|  |  |
| --- | --- |
| 基线项名称 | 密码复杂性设置 |
| 检查步骤 | 在管理工具打开本地安全策略，依次打开：安全设置—帐户策略—密码策略，检查密码必须符合复杂性要求与密码长度最小值两项设置 |
| 基线合规性判定 | 已启用密码必须符合复杂性要求且密码长度最小值为8及以上即合规，否则不合规 |
| 加固步骤 | 在管理工具打开本地安全策略，依次打开：安全设置—帐户策略—密码策略  启用密码必须符合复杂性要求，并设置密码长度最小值为8。 |

|  |  |
| --- | --- |
| 基线项名称 | '强制密码历史'设置为5-24之间 |
| 检查步骤 | 在管理工具打开本地安全策略，依次打开:安全设置—帐户策略—密码策略，检查强制密码历史是否大于等于五 |
| 基线合规性判定 | 已启用强制密码历史且值大于等于五即合规，否则不合规 |
| 加固步骤 | 在管理工具打开本地安全策略，依次打开:安全设置—帐户策略—密码策略  将强制密码历史设置为5-24之间，推荐为5 |

|  |  |
| --- | --- |
| 基线项名称 | 配置账户锁定策略 |
| 检查步骤 | 在管理工具打开本地安全策略，依次打开:安全设置—帐户策略—账户锁定策略，检查账户锁定阈值，账户锁定时间和重置账户锁定计数器 |
| 基线合规性判定 | 账户锁定阈值设置为3-8之间且账户锁定时间和重置账户锁定计数器设置为10-30之间即合规，否则不合规 |
| 加固步骤 | 在管理工具打开本地安全策略，依次打开:安全设置—帐户策略—账户锁定策略。  将账户锁定阈值设置为3-8之间，建议值为5，输错5次密码锁定账户；  将账户锁定时间和重置账户锁定计数器设置为10-30之间，建议值为15，账户锁定时间为15分钟。 |

|  |  |
| --- | --- |
| 基线项名称 | 配置安全选项账户策略 |
| 检查步骤 | 在管理工具打开本地安全策略，依次打开:安全设置—本地策略—安全选项。检查"账户：来宾账户状态"，"账户：使用空密码的本地账户只允许控制台登陆" |
| 基线合规性判定 | "账户：来宾账户状态" 设置为:已禁用，"账户：使用空密码的本地账户只允许控制台登陆"设置为:启用即合规，否则不合规 |
| 加固步骤 | 在管理工具打开本地安全策略，依次打开:安全设置—本地策略—安全选项。  将"账户：来宾账户状态"设置为:已禁用  将"账户：使用空密码的本地账户只允许控制台登陆"设置为:启用。 |

|  |  |
| --- | --- |
| 基线项名称 | 密码使用到期修改提醒 |
| 检查步骤 | 在管理工具打开本地安全策略，依次打开:安全设置—本地策略—安全选项。检查”交互式登录：提示用户在过期前修改密码” |
| 基线合规性判定 | 提示时间设置为5到14天之间即合规，否则不合规 |
| 加固步骤 | 在管理工具打开本地安全策略，依次打开:安全设置—本地策略—安全选项。将 ”交互式登录：提示用户在过期前修改密码”设置为5到14天之间 |

|  |  |
| --- | --- |
| 基线项名称 | 匿名账户访问控制 |
| 检查步骤 | 在管理工具打开本地安全策略，依次打开:安全设置—本地策略—安全选项。检查下列四项的配置情况  “Everyone权限应用于匿名用户“  “不允许SAM帐户的匿名枚举“  “不允许SAM帐户和共享的匿名枚举”  ”允许匿名SID/名称转换“ |
| 基线合规性判定 | 将“Everyone权限应用于匿名用户“设置为：已禁用  将“不允许SAM帐户的匿名枚举“设置为：已启用  将“不允许SAM帐户和共享的匿名枚举”设置为：已启用  将”允许匿名SID/名称转换“设置为：已禁用。  即合规，否则不合规 |
| 加固步骤 | 在管理工具打开本地安全策略，依次打开:安全设置—本地策略—安全选项。  将网络访问中“Everyone权限应用于匿名用户“设置为：已禁用  将“不允许SAM帐户的匿名枚举“设置为：已启用  将“不允许SAM帐户和共享的匿名枚举”设置为：已启用  将”允许匿名SID/名称转换“设置为：已禁用。 |

|  |  |
| --- | --- |
| 基线项名称 | 设置空闲会话断开时间 |
| 检查步骤 | 在管理工具打开本地安全策略，依次打开:安全设置—本地策略—安全选项。检查 Microsoft网络服务器中的"暂停会话之前所需的空闲时间数量"、"登陆时间过期后断开与客户端的连接" 的配置情况 |
| 基线合规性判定 | Microsoft网络服务器中的"暂停会话之前所需的空闲时间数量"设置为:5-30之间，"登陆时间过期后断开与客户端的连接"设置为:已启用 即合规，否则不合规 |
| 加固步骤 | 在管理工具打开本地安全策略，依次打开:安全设置—本地策略—安全选项。  将Microsoft网络服务器中的"暂停会话之前所需的空闲时间数量"设置为:5-30之间，建议值为15  将"登陆时间过期后断开与客户端的连接"设置为:已启用 |

|  |  |
| --- | --- |
| 基线项名称 | 禁止未登录强制关机 |
| 检查步骤 | 在管理工具打开本地安全策略，依次打开:安全设置—本地策略—安全选项。检查 "关机:允许在未登录时关闭系统" 的配置情况 |
| 基线合规性判定 | 关机:允许在未登录时关闭系统"设置为:已禁用即合规，否则不合规 |
| 加固步骤 | 在管理工具打开本地安全策略，依次打开:安全设置—本地策略—安全选项。  将"关机:允许在未登录时关闭系统"设置为:已禁用 |

|  |  |
| --- | --- |
| 基线项名称 | 检查注册表自启动项 |
| 检查步骤 | 打开注册表编辑器，检查项注册表路径HKEY\_LOCAL\_MACHINE\\SOFTWARE\\Microsoft\\Windows NT\\CurrentVersion\\Winlogon的Userinit中可疑启动项 |
| 基线合规性判定 | 不存在无法确定的启动项即合规，否则不合规 |
| 加固步骤 | 打开注册表编辑器，检查项注册表路径HKEY\_LOCAL\_MACHINE\\SOFTWARE\\Microsoft\\Windows NT\\CurrentVersion\\Winlogon的Userinit中的危险启动项并删除，注意不要删除系统默认启动项C:\\Windows\\system32\\Userinit.exe |

**其他配置**

|  |  |
| --- | --- |
| 基线项名称 | 检查可关闭系统的帐户和组 |
| 检查步骤 | 在管理工具打开本地安全策略，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\用户权限分配”，在右边窗格中找到“关闭系统”，检查配置情况 |
| 基线合规性判定 | 配置仅含有“Administrators”用户组即合规 |
| 加固步骤 | 在管理工具打开本地安全策略，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\用户权限分配”，在右边窗格中找到“关闭系统”，配置为仅含有“Administrators”用户组 |

|  |  |
| --- | --- |
| 基线项名称 | 检查可从远端关闭系统的帐户和组 |
| 检查步骤 | 在管理工具打开本地安全策略，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\用户权限分配”，在右边窗格中找到“从远程系统强制关机”，检查配置情况 |
| 基线合规性判定 | 配置仅含有“Administrators”用户组即合规 |
| 加固步骤 | 在管理工具打开本地安全策略，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\用户权限分配”，在右边窗格中找到“从远程系统强制关机”，配置为仅含有“Administrators”用户组 |

|  |  |
| --- | --- |
| 基线项名称 | 检查是否已启用“不显示最后的用户名”策略 |
| 检查步骤 | 在管理工具打开本地安全策略，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“登录屏幕上不要显示上次登录的用户名”(适用于Windows2000)或“交互式登录: 不显示最后的用户名”，检查配置情况 |
| 基线合规性判定 | 配置仅含有“Administrators”用户组即合规 |
| 加固步骤 | 在管理工具打开本地安全策略，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“登录屏幕上不要显示上次登录的用户名”(适用于Windows2000)或“交互式登录: 不显示最后的用户名”，配置为“已启用”。 |

|  |  |
| --- | --- |
| 基线项名称 | 检查“锁定会话时显示用户信息”级别 |
| 检查步骤 | 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”检查是否存在名称为“DontDisplayLockedUserId”、类型为DWORD的值，若已存在则检查其数据是否为3。  （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。） |
| 基线合规性判定 | DontDisplayLockedUserId数据为3即合规 |
| 加固步骤 | 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为3。 |

|  |  |
| --- | --- |
| 基线项名称 | 检查是否已对所有驱动器关闭Windows自动播放 |
| 检查步骤 | 在管理工具打开本地安全策略，浏览到路径“本地计算机策略\计算机配置\管理模板\Windows组件\自动播放策略”(适用于Windows2008、WindowsVista、Windows2008R2、Windows7)或“本地计算机策略\计算机配置\管理模板\系统”(适用于Windows2000、WindowsXP、Windows2003、Windows2003R2)，在右边窗格中找到“关闭/停用自动播放”，配置为“启用”，检查是否为对“所有驱动器”生效。 |
| 基线合规性判定 | 设置为对“所有驱动器”生效即合规 |
| 加固步骤 | 在管理工具打开本地安全策略，浏览到路径“本地计算机策略\计算机配置\管理模板\Windows组件\自动播放策略”(适用于Windows2008、WindowsVista、Windows2008R2、Windows7)或“本地计算机策略\计算机配置\管理模板\系统”(适用于Windows2000、WindowsXP、Windows2003、Windows2003R2)，在右边窗格中找到“关闭/停用自动播放”，配置为“启用”，且选为对“所有驱动器”生效。 |