🗩 禁止云桌面用户修改IP地址

张玉玺 2019-12-23 发表

组网及说明
无
配置步骤
思杰云桌面基于微软域控工作,对于MCS专有桌面,不授予用户管理员权限,某些程序考嫩恶搞无法运行,安装软件也会受阻,授予管理员权限后,用户可能会自行修改桌面IP地址、DNS信息,导致桌面连接中断,无法登陆桌面等问题,本文介绍如何通过域组策略设置,禁止具有云桌面本地管理员权限的用户修改桌面网络配置的方法。

1. 打开AD上的服务器管理器,点击工具-组策略管理;

📥 服务器管理器		- 0 ×
€ ● ● ■ 服务器管	管理器・仪表板	◆ ② │
	欢迎使用服务器管理器	Active Directory 站点和服务 ADSI 编辑器
■ 本地服务器 ■ 所有服务器 ■ AD DS	● 服务器管理器・仪表板 ● <th< td=""></th<>	
品 DNS ■ 文件和存储服务 ▷	快速启动(Q) 2 添加角色和功能	ODBC 数据源(64 位) Windows PowerShell
	3 添加要管理的具他服 新 ^{编功能(W)} 4 创建服务器组	Windows PowerShell ISE Windows PowerShell ISE Windows PowerShell ISE (x86)
	5 将此服务器连接到云	Windows Server Backup 形 Windows 内存诊断 本地安全策略
	用巴和服为品約1 角色:3 服务器组:1 服务器总数:1	高級安全 Windows 防火場
	AD DS 1	任务计划程序 事件查看器
	① 可管理性 ① 可管理性 事件 事件 事件	碎片整理和优化驱动器 系统配置
	服务 服务 性能 性能	系统信息 性能监视器 用于 Windows Downs Chall 00 A stice Disasters 開始
	BPA 结果 BPA 结果	用于 Windows PowerSheir as Active Directory tax 资源监视器 编集器管理
		组件服务 1925 —
- P 🗆 😂	🚽 🛹 🚠 陆 🗁 📠	1日 小 二 日本 1月 日本 1

2. 在左侧的目录上上,找到想要限制修改ip的计算机所在的组织单元,右击,选择"在这个域中创建一条 GPO并链接到此处",此组织单元的所有计算机将受到策略限制而不能修改IP地址;



3. 为这条策略拟定一个名称,本例输入"禁止用户修改IP地址",点击确定;

▲ 組策略管理 ▲ 文件(F) 操作(A) 查看(V) 窗口(W) ◆ ● ▲ ② □ □ ▲ ※ □ ④ ■ ▲ 細節幣管理 × A 林: bountab	帮助(H) Desktops KHED/MI2ER/H-M, GOLERDAN-S, H. H.	- 0 ×
 ◆ At rsyunab ◆ 副 hsyunlab ◆ 副 hsyunlab ◆ 圖 Ctrix ② Desktops > ③ Users > 圖 Domain Controllers > 圖 MM 指因器 > Stater CPO 	社研研究和本地公園、 須賀和製地水	域
> 論 就在 資 追策略建構 覺 追策略结果	<u>多称(N):</u> 薬止用产修改(P地址 遅 Starter GPO(S): (元) ~	2
#	🗢 1 🖡 🎮 🍯	19:31

4. 在所选择的OU下,找到刚才创建的策略,右击,选择"编辑"

🔜 组策略管理		– Ø X
🔜 文件(F) 操作(A) 查看(V) 窗口(W) 🕯	曲(H)	- 8)
🗢 🔿 🙍 📰 💥 🙆 🔢 📷		
通 組錬略管理 > ▲ 純 hsyun.lab > ● 前 hsyun.lab > ② Cirix > ② Cirix > ③ Lirix > ③ Domain Contro > ④ Users > ⑤ Users > ⑤ Users > ⑤ With 尚法務 > ⑤ Stater GPO ※ 協振 ※ 個振聴建構 ※ 細振聴編集	禁止用户修改IP地址 作用域 详细信息 设置 委派 留着 在此位置向显示链接(L): 下列站点,域和違以单位链接到此 GPO(T): 運動 直 課題 日用 注意 第 時期(L): 第 日用 第 日 第 日 第 日 第 日 第 日 日 第 日 日 第 日 第 日	~
Ling Minister, 删除(C)) (M)	
	, Units [液如(D) 對除(R) 居性(P)	
	¥11 90 A 此 GPO 田接到下列 WMI 橫透離(W): ≪无> ✓ 打开(0)	ф 19:34

5. 依次展开"计算机配置-策略-windows设置-安全设置",双击"系统服务";



7. 删除现有的安全组和用户



8. 点击"添加",输入"Domain Admins",点击检查名称,正确解析后,点击确定;

			40(8	_
主波直 Network Connections		r A	1XFR 2Dectroly	
安全			次有定义 沿右完 ○	
组成田内文(6)。			没有定义	
所有组或用户均不具有访问此对象的	的权限。但是该对	象的所有者 ^	选择用户、计算机、服务帐户或组	>
可以分離的以限。			选择此对象类型(S):	
			用户、组或内置安全主体 对象类型(0))
			查找位置(F):	
L	活加(D)	₩/ke/(R)	hsyun.lab 位置(L)	
	/84/JH(D/)	(21)251026	输入对象名称来选择(示例)(E):	
权限	允许	拒绝	Domain Admins 检查名称(C	.)
完全控制		· ^		
读取				
启动、停止和暂停				
写入			高級(4) 通完 取送	
删除			INDUCTION INTO A PROPERTY OF A	
*********		~	没有定义 编辑安全设置(E)	
有关特殊权限或高级设置,请单击"?	高级"。	高级(V)	没有定义	
			没有定义	
			没有定义	
			没有定义	
确完	取満	応用(Δ)	没有定义	
	-0.01	1201000	没有定义 确定 取消 应序	∄(A)
10 HOLL (QR	emote Desktop	Servic 没有定义	没有定义	
	emote Desktop	Servic 没有定义	没有定义	
> 🖄 R	emote Procedur	re Call 没右完义	沿右完♡	

9. 选中新添加的"Domain Admins",勾选"完全控制",是的域管理员具有修改IP地址的完全控制权限;



10. 重复步骤8和9, 添加"Everyone"用户, 仅勾选"读取"权限; 点击确定, 关闭窗口;

 ・課目用時数1P時地(CTXAI ^ 第4 ・第4 ・第4 ・第4 ・第 ・第 ・第		93778 ?	×	
	LVeryone	nain Admins)	tions 届性 vork Connections	? ×
→ 通 本地策略 ● 通 要求相当本 ● 通 要求規制的 ● 通 要規制的 ● 通 要規制的 ● 通 素統服務 ● 通 素統服務 ● 通 素統服務 ● 通 素統服務 ● 通 素統服務 ● 通 和能限者 ● 通 和能用者 ● 通 和能用者 ● 通 和能用者 ● 通	Everyone 的权限(P) 完全控制 退取 目动、停止印智停	添加(D) 謝除(R)	2篇(D) 动模式:	
 > 22 大規模相(22 大規模相(23 大規模相(24 大規模相(24 大規模相(25 広用程序 26 正用程序 26 正規定兼明 26 正規定兼明 26 正規定兼解的(27 正規定 27 正規定 28 正規定 29 正規定 29 正規定 20 正規定 20 正規定 20 正規定 20 正規定 25 正規定 26 正規定 27 正規定 27 正規定 28 正規定 29 正規定 20 正規定<td>马入 劃除 </td><td>口 口 口 一 一 一 一 一 一</td><td>⁵) 全设置(E)</td><td></td>	马入 劃除 	口 口 口 一 一 一 一 一 一	⁵) 全设置(E)	
→ <i> ☆ 第 ☆ 第</i>	発定 Remote Desktop Servic 没有定义 Remote Procedure Call 没有定义	取消 应用(A) 没有定义 没有定义	确定	取消 应用(A)

11. 点击"确定",关闭策略设置窗口;



12. 任意找一台隶属于策略应用范围内的一台虚拟机,打开命令行,输入"gpupdate /force",等待策略更新 完成,重启计算机;



13. 右击通知栏的网络图标,右击,选择"打开网络和共享中心",可以发现原来的网络连接已经隐藏;



14. 点击"更改适配器连接",所有的网络适配器也被隐藏,因而用户将不能自行更改IP地址、DNS等网络设置;



15. 在开始菜单输入"services.msc",启动服务管理器,找到"Network Connections",右击该服务,发现" 启动"按钮不可用,说明当前用户没有权限启动该服务;

Network Connections	名称		描述	状态	启动类型	登录为	
	Alicrosoft .NET Framewo	ork NGEN v2	Microsoft .NET Frame		禁用	本地系统	
描述:	Microsoft .NET Framework NGEN v4 Microsoft .NET Framework NGEN v4 Microsoft iSCSI Initiator Service Microsoft Software Shadow Copy Pr		Microsoft .NET Frame		自动(延迟 自动(延迟 禁用 手动 自动 禁用	本地系统	
管理 "网络和拨号连接" 文件夹中对			Microsoft .NET Frame			本地系统	
象,在其中您可以查看局域网和远程 连接。			管理从这台计算机到远…			本地系统	
连接。			管理卷影复制服务制作			本地系统	
	🔍 Multimedia Class Schedu	基于系统范围内的任务…		本地系统 网络服务			
	🔍 Net.Msmq Listener Adap	Receives activation re					
	🔍 Net.Pipe Listener Adapte	Receives activation re Receives activation re Provides ability to sha 为用户和服务身份验证		禁用	本地服务		
	State of the second			禁用	本地服务		
			已启动	禁用	本地服务		
				自动	本地系统		
	🔍 Network Access Protecti	on Agent	网络访问保护(NAP)代		手动	网络服务	
	🐫 Network Connectio	启动(S)	网络和拨号连接		手动	本地系统	
	🔍 Network List Service	信止(0)	算机已连接的网	已启动	自动	本地服务	
	🔍 Network Location A	(学生(0)	存储网络的配置	已启动	自动	网络服务	
	🔍 Network Store Inter		向用户模式客户	已启动	自动	本地服务	
	🔍 Offline Files	秋夏(M) 赤蛇白动(D)	:件服务在脱机文		禁用	本地系统	
	Real Controls	里新启动(E)	是 Vista 中的 Wi		手动	本地服务	
	Reer Name Resolut	所有任务(K)	▶ 等名称解析协议(手动	本地服务	
	Reer Networking G	层(金斤(F)	等分组启用多方		手动	本地服务	
	🔍 Peer Networking Id	Algori (C)	名称解析协议(P		手动	本地服务	
	Reversion Performance Count	屆性(R)	用户和 64 位进		手动	本地服务	
	Performance Logs &	帮助(H)	志和警报根据预		手动	本地服务	
	🔍 Plug and Play		。,机在极少或没有…	已启动	自动	本地系统	
	Operation Property of the second s	r	PnP-X 总线枚举器服务		手动	本地系统	
	Section 2018 PNRP Machine Name Pu	blication Ser	此服务使用对等名称解		手动	本地服务人	_

配置关键点

注意:

- 1. 本配置案例将该策略链接到"Desktop"所在组织单元,该组织单元中的所有计算机将在下次重启后应用 该策略;
- 被策略修改的是计算机配置,仅对计算机生效,任何用户(除域管理员)登录该计算机都将无法设置 网络,若将该策略应用到用户所在的组织单元,该策略将不生效;
- 3. 停止"Network Connections"服务并不影响这台计算机正常获取DHCP地址,与其他计算机通信等