

	目	R
文档信息	错误!未定义书签。	
		0/
第1章	概述	
1.1	实施概述	2
1.1.1	关于委派控制	2
1.2	实施准备	2
1.3	实施目标	2
1.4	实施思路	2
第 2 章	实施步骤	3
2.1	安装 AD 远程管理工具	3
2.1.1	安装 KB958830 补丁包	
2.1.2	安装 AD 远程管理模块	
2.2	委派控制	7
2.2.1	委派步骤	7
2.2.2	委派控制的本质	
第3章	QA	
3.1	Exchange 2010 角色无法安装	错误!未定义书签。



第1章 概述

1.1 实施概述

本文档依据 Exchange 2007 邮件系统升级项目实施准备条件要求,委派各分行管理员进行指定权限的 AD 管理,本文是根据该项目实施过程标准及规范形成该文档。

1.1.1 关于委派控制

委派范围: 在 AD 中可以委派控制的范围是站点、域、和组织单位合称为: SDOU 从管理层面来看,不同的委派范围涉及不同的性质工作。例如: 站点上最主要工作就是 新建、删除站点、网站连接、子网络等项目。组织单位上最常见的工作,通常是新建、删除 用户和计算机帐户、重设密码与应用组策略等。所以说,委派的范围有两重意义,第一,它 界定了管辖权的范围,就是说被委派的对象只允许在此范围内行使管理权,第二,它提示了 不同性质的工作属性,我们应当针对不同的范围委派的工作。

委派对象: 在从多 AD 对象中只有用户、计算机和组可以作为委派控制的对象,此外, 该对象不必和授权范围有任何隶属关系。例如: 可以将 A 组织单位委派给 B 组织单位的成 员管理,甚至可以委派给其它域的用户管理。

1.2 实施准备

准备客户端管理机及服务器远程管理工具安装包。客户端管理机须加域

1.3 实施目标

在当前分支机构,如北京、上海、福州等,部署了额外域控,。

1.4 实施思路

- 1) 准备一台管理操作主机,安装管理工具。
- 2) 设置管理员相应权限。
- 3) 派发管理 ou 的控制台文件。



第2章 实施步骤

2.1 安装 AD 远程管理工具

[提示:为了避免活动目录域管理员登录后的 token 被窃取攻击的可能性,用户活动目录域 AD 远程管理的这台计算机一定要确保它的安全,这可能包括物理隔绝。]

2.1.1 安装 KB958830 补丁包

双击安装程序



弹出提示是否安装 KB958830 补丁,选择"是"进行安装

Windows	Windows Update 独立安装程序
正在此计	您要安装以下 Windows 软件更新吗? Windows 更新程序 (KB958830)

选择"我接受",进行更新安装

阅读这些许可条款(安装更新前,要求您接受许	第 1 条,共 _{可条款。}	(1条)		
Mindows 更新程序(KB958830)				
MICROSOPT软件许可条款 MICROSOPT REMOTE SERVER ADMINI 本许可条款是 Microsoft Corpora 公司) 与您之间达成的协议。请阅 来接收该软件的媒体(若有)。本 述内容附带有其他条款): • 更新、 • 补充、 • 量于 Internet 的服务和 • 支持服务 如果确实附带有其他条款,则其他	STRATION TOOLS 1 tion (或您所在地 卖本条款的内容。 条款也适用于 Mio 条款应适用。	FOR WINDOWS 7 的 Microsoft (本条款适用于上 crosoft 为此软)	SP 1 Corporation 关瞭 计,其中包括您 并提供的(除非下	1



等待安装完成,点击"完成"退出。



2.1.2 安装 AD 远程管理模块

(1) 安装完 KB958830 后,打开"控制面板"







(3) 选择"打开或关闭 windows 功能"

控制面板 🕨	程序)	▼ 49 搜索控制面板
et	ø	程序和功能 卸载程序 ③打开或关闭 Windows 功能 查看已安装的更新 运行为以前版本的 Windows 编写的程序 如何安装程序
	•	默认程序 更改媒体或设备的默认设置 始终使用指定的程序打开此文件类型 设置默认程序
区域		桌面小工具 向桌面添加小工具 联机获取更多小工具 卸载小工具 还原 Windows 上安装的桌面小工具
(4)	在"远程	管理工具"中添加需要的服务,在这里我们添加"AD管理工具"。
	🕅 Windo	ws 功能
	打开或 若要打开 框。 填充	关闭 Windows 功能
		远程服务器管理工具 人名法 化分子子 化分子子 化分子子 化分子子 化分子子 化分子子 化分子子 化分子
	6	8 回 🦆 Active Directory 证书服务工具 9 回 🐌 AD DS 和 AD LDS 工具
		 □ □ ▲ AD DS 工具 □ ▲ Active Directory 管理中心 □ ▲ AD DS 管理单元和命令行工具 □ ▲ AD DS 管理单元和命令行工具 □ ▲ AD LDS 管理单元和命令行工具
1		■ 用于 Windows PowerShell 的 Active Directory +
		确定取消



(5) 点击确定后,进行工具安装。

	大团 WINDOWS 切能 一种功能 法法权官复法据 英莱兰伊一种功能 法法	****
Micros	soft Windows	
Wir 要厂	ndows 正在更改功能 , 请稍候。这可能需 1分钟。	
	☑ ▲ AD DS 管理単元和命令行工具 ☑ 用于 NIS 工具的服务器	E
	□ → AD LDS 管理单元和命令行工具	
	🕖 用于 Windows PowerShell 的 Active Dir	ectory 🚽

(6) 选中之后确定添加,添加完毕后,再点击开始,在管理工具中就可以看到 AD 的 相关管理工具了





(7) 打开 "Active Directory 用户和计算机",即可浏览到域控信息。

Active Directory 用户和计算。 名称	東型	編送	
97760256 Builtin 9 Builtin 9 Builtin 9 Computers 9 Domain Controllers 9 LoadGen Objects 9 LoadGen Objects 9 Managed Service A 9 Octs2007 9 Servers 9 Test to domino 9 XIIL 9 XIIL 9 XIIL	 builtinDoma 容器 温沢単位 道沢単位 道沢単位 道沢単位 道沢単位 三 容器 道沢単位 三 容器 道沢単位 三 電器 正 道沢単位 正 道沢単位 取(中位 	in Default container for Default container for Default container for Generated by LoadGen Default container for	

2.2 委派控制

2.2.1 委派步骤

这里以 BJDAG 帐号对北京分行的组织单元进行管理员权限委派为例。

(1)	启动"Active	Directory 用,	户和计算机"	(ADUC),	找到需要委派的 OU	: 北京分行
-----	-----------	--------------	--------	---------	------------	--------

			2204 optic 2
🗉 🗐 全行计算机	 名称 		类型
	\$~\$	r (支行)主管 (支行)主管AB角 (文件接收人 管理部_user 线工作小组 控制部_user 委员会 导 同业部	安全组 - 通用 安全泊 - 通用 安全讯 - 通通用 安全讯 - 通通用 安全全 - 一一一一一一一一一一一一一一一一一一一一一一一一一一一一一一一一一一
E 2	198 S	间业部_user 业务小组	用户 安全组 - 通用



(2) 右击"北京分行"OU,选择菜单:委派控制

□ == ↔ IC/R/ □ = = □ = = 上海	· ř 分行	▲北京分 ▲北京分 ▲北京分
日 🗎 北京	公行 委派控制 (R)	4 1 1 京分
	移动(V) 查找(I)	(京) (京) (京)
+ 1 + 1 + 1	新建 (N) 所有任务 (K)	▶ 京分 ▶ 京分
E 🗐	查看(V)	▶ 凉分
E	剪切(T)	惊

(3) 进入委派控制的配置向导

控制委派向导	
	欢迎使用控制委派向导
P	此向导帮助您委派对 Active Directory 对象的控制。 可以给予用户权限来管理用户、组、计算机、组织单位 和其他存储在 Active Directory 域服务中的对象。
	单击"下一步"继续。
	<上一步 (B) 下一步 (D) 》 取消 帮助
(4) 点击"下一步"	



控制委派向导	X
用户或组 选定一个或多个您想委派控制的用户或组。	
选定的用户和组 (2):	
添加 (4)	
< 上一步 (2) 下一步 (2) > 取消 帮助	

(5) 点击"添加(A)"按钮,选择需要指派的用户:

选择用户、计算机或组	? ×
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 (E):	
. en	
输入对象名称来选择(<u>示例</u>)(2):	
BJDAG (BJDA	检查名称 C)
高级(4)	确定 取消

(6) 点击"确定",并进入下一步,在此我们选择创建自定义任务去委派:

控制委派向导	×
要委派的任务 您可选择常见任务或自定义您自己的任务。	R
○ 委派下列常见任务 @):	
 □ 管理组策略链接 ▲ 生成策略的结果集(计划) 	
 □ 生成策略的结果集(记录) □ 创建、删除和管理 inetOrgPerson 帐户 □ 重置 inetOrgPerson 密码并强制在下次登录时更改密码 □ 读取所有 inetOrgPerson 信息 	
● 创建自定义任务去委派 C)	
< 上一步 @) 下一步 @) > 取消	帮助



(7) 在出现 ad 对象类型选择,选择只是在这个文件夹中的下列对象

用户、组、组织单元三项,并点击"下一步"
控制委派向导
Active Directory 对象类型选择 Image: Figure Directory 对象类型选择 Image: Figure Directory Direc
委派以下对象的控制:
○ 这个文件夹,这个文件夹中的对象,以及创建在这个文件夹中的新对象 Œ)
 只是在这个文件夹中的下列对象 (0):
 □ 打印机 对象 □ 用户 对象 □ 站点 对象 □ 站点容器 对象 □ 站点设置 对象
 □ 在这个文件夹中创建所选对象 ©) □ 删除这个文件夹中的选择的对象 @)
< 上一步 (B) 下一步 (B) > 取消 帮助
④ 只是在这个文件夹中的下列对象 (0):
▲ 站点链接桥 对象
▶ 2 1 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2
□ ↓ 计算机 对象

(8) 点击下一步,将权限设为完全控制

控制委派向导			×
权限 选定要委派的权限。		?	
显示这些权限:			
▼ 常规(G)			
□ 特定属性 @)			
□ 特定子对象的创建	/刪除(C)		
权限 (E):			
☑ 完全控制		_	
☑ 读取 ☑ 写入			
☑ 创建所有子对象			
☑ 删除所有子对象			
		<u> </u>	
	〈上一步®〉下一步®〉	取消 帮助	

(9) 点击"下一步"完成控制委派向导:



制委派向导	
	完成控制委派向导
R	您已成功地完成控制委派向导。
	您选择在下列 Active Directory 文件夹中 ▲ 委派对象的控制:
	■ •. en/[· · · · · · · · · · · · · · · · · · ·
	您所给予控制的组、用户或计算机是:
	BJDAG (BJDA
	它们有下列权限:
	完全控制
	'若要关闭此向导,请单击"完成"。
	< 上一步 (8) 二二 二 二 二 二 二 二 二 二 二 二 二 二 二 二 二 二 二
	1. S.

2.2.2 委派控制的本质

AD 委派控制本质就是修改 AD 对象中的 ACL, 使委派的对象具有相符的权限。 查看委派: 启动 ADUC 的高级功能,选择"查看"-"高级功能"

Active Direct	ory 用户和计算机		_ 🗆 🗙
文件(P) 操作(A)	查看(V) 帮助00		
(* * 2 m	[添加/删除列 (A)	2 %	
 E Users E 上海分行 E 2 全行计算 E 3 其他用户 	大图标(G) 小图标(M) 利表(L) ・详细信息(D)		A
	用户、联系人、组和计算机作: ✓ 高级功能(V) 締选器选项(F) 自定义(0)	5容器 (C)	
	Image: Constant of the second	ce Accounts hange Security Groups hange System Objects	
H 🗃 Microsof H 📑 Microsof	ft Exchange		×
启用/禁用高级功能和	叼建	1	

右击委派的 OU, 选择"属性"



	委派控制 (2) 移动 (V) 查找 (2)	mputers main Controllers mino reignSecurityPrincipa
5 🚊 19 5 🗐 19 5 📓 19	新建 (M) 所有任务 (K)	<pre>> frastructure ></pre>
	剪切(T) 删除(D) 重命名(M) 刷新(F)	adGen Objects stAndFound maged Service Account crosoft Exchange Secu
E 🗐 🦻	属性 (R)	DS Quotas
• 🖬 🕽	帮助 00	12007 Trogram Data

在弹出的属性选项中,选择"安全"选项卡:

_

BjDag (Bji	0		×
& Exchange Services	(a)	6	-
3	1	in-reason fi	<u>•</u>
BJDAG 的权限(E)		<u></u>	拒绝
完全控制 读取			
与入 创建所有子对象 删除所有子对象			
有关持殊权限或高级设置,	请单击"派	馺"。	高级创

选取安全选项卡中的"高级"属性来验证委派的 ACL,我们可以查看到 BJDAG 配置了关于"组"/"组织单位"/"用户"三个权限项目



	? ×			- OX		
属性编辑器	校開 一 東京香	■100022244000 軍後 所有者 有效权限 成績績权限项目的详细信息。	 - 通选择该项目并单也	"编辑"。		
ervices) 版型) 機能和 方式许 拒绝 日 日 日 日 日 日 日 日 日	1 1 2 1 1 1	ETDAG BJDAG	(校課) 特殊 特殊 特殊 回識/制除 计 回識/制除 任 回識/制除 任 可識/制除 用 完全控制 特殊 完全控制	- 建築子	広用于 后代 組 対象 后代 組织単位 対象 后代 用户 対象 只是这个对象 只是这个对象 只是这个对象 只是这个对象 只是这个对象 只是这个对象 只是这个对象 只是这个对象 只是这个对象 只是这个对象	1
· [_ ـ ـ ـ ـ ـ ـ ـ ـ ـ ـ ـ ـ ـ ـ ـ ـ ـ ـ		00」编辑 20 司从该对象的文项继承的权 型项目	 (0) (0)			

选中对应的权限项目,点击"编辑"按钮,显示委派工作的内容。

应用于(0): 后代 用户 对象		-
权限 (£):	允许	拒绝
元主任的 列出内容 属性 写入全部属性 删除 删除子树目录 读取权限 修改权限 修改机有者 所有验证的写入 所有扩展权限	<u></u>	

2.2.3 删除管理员

委派控制向导有一个缺点:只能够用来建立委派工作,但是无法删除或更改委派工作, 如果要取消或更改授权的人选或者工作属性,则必须直接修改该对象的 ACL。

删除方法: 右击对应的 OU 打开其属性, 切换到"安全"选项卡, 再按编辑就可以修改 委派的权限, 或者点击删除按钮

(1) 右键单击选中需要删除管理员的组织单元,选择属性



分行 委派控制 (2) 移动 (V) 査找 (2)	名称 Builtin mputers main Controllers mino reignSecurityPrincips
新建(A) 所有任务(K) 剪切(T) 删除(D) 重命名(M) 刷新(P)	adGen Objects stAndFound maged Service Account crosoft Exchange Secu
属性 (B) 帮助 00	crosoft Exchange Syst DS Quotas s2007 Frogram Data

(2) 在弹出的属性选项中,选择"安全"选项卡

🖁 BJDAG (
2 . REExchange Services (- A)			
I	4			-	
		添加①	制余区		
JDAG 的权限 (£)		允许	拒绝		
完全控制		8	8	-	
写入			H		
创建所有子对象					
關係所有子对象				-	

(3) 选中要删除的管理员,点击删除即可。最终点击确定。

A MT		ĩ	
BJDAG (
2 陈 2 陈	(a		
A.		添加(2)	HH R CB



2.3 委派用户管理方式

使用服务器远程管理工具登录

自定义 MMC 限定 OU 访问控制

方法:将 Active Directory用户和计算机(ADUC)的 mmc 进行自定义,只把委派用户管理的 OU 列出,保存后发送给此用户,然后将 ADUC 所需的文件拷贝的客户端,此用户就可以管理特定 OU 而无法浏览到其他 OU。

(1) 在 DC 上,点击开始-运行,输入 mmc,确定。

📨 运行		×	
「空 Windows) 文件実、文	将根据您所输入的名称,为 档或 Internet 资源。	您打开相应的程序、	
打开(<u>O</u>): mmd		-	
,		_	
Γ	确定 取消	〕 浏览(B)	
 添加 ADUC 管理单元			
	··		
● 控制音1 - L控制	ゴ根で点」		
🔁 文件 (P) 操作 (A)	· 查看(V) 收藏夹(0)		
🧼 新建 (N)	Ctrl+N		
┌── 打开 (0)	Ctrl+0		
保存(S)	Ctrl+S		
添加/删除管理单	单元(M) Ctrl+M		
选项(P)			
1 tsadmin			
2 dsa			
3 dr.smgmt			
4 dssite			



100

Т

 可用的管理单元 (S): 管理单元 Active Directory 用户 Active Directory 域和 Active Directory 站点 ActiveX 控件 ADSI 编辑器 DNS IP 安全策略管理 IP 安全监视器 	供应商 Microsod Microsod Microsod Microsod Microsod Microsod Microsod Microsod Microsod Microsod Microsod Microsod Microsod	添加(&) >	所选管理单元 @): 登制台根节点 Active Directory 用户和计算机	- 編辑扩展 &) 開除 ® 上移 W 下移 ®
Windows Server Backup 描述: Active Directory 用户和计算机	Microsol▼ 」 可以管理用户	、组、组织单	▲) 位和其他所有 AD DS 对象。	- 高級 (⊻)

找到将委派给用户的 OU, 右键单击选择 从这里创建窗口。将显示整个域的窗口关闭, 只留下特定 OU 的窗口。

🧱 控制台1 - 〔控制	台根节点\Active Di	rectory 用户和计算机 📥	
🚡 文件 (F) 操作 (A) 查看(V) 收藏夹	0) 窗口(#) 帮助(H)	
🇢 🔿 🙋 🚾 😼	K 🗖 🔀 🗔 🙆	3 🛛 🖬 🔧 🐮 🦷	2 B
 田 21 其他用户 田 21 上海分行 	▲ <u>名称</u> 泉 え		★ Office Communicatios ▲
	要派控制 (2) 容动 (Y) 查找 (1) 新建 (X) 所有任务 (X) 查看 (Y) <u>从这里创建窗口 (Y)</u> 新任务板视图 (T) 剪切 (T) 删除 (D) 重命名 (M) 刷新 (P) 导出列表 (L)	· · · · · · · · · · · · · · · · · · · · · · · · · · · · · · · · · · · · · · · · · · ·	
▲ 在这个节点上打开新	興性 (R) 帮助 (H)		



北京分行				- FOR POLITI			1	
北京分行		名称	夫型	橫述	*	操作		
夺制台根节点\Act	ive Dir	ectory IIPani					0	×
※ 2 其他用户	-	名称	大型 中心的 - 通用	描述	-	操作	- 1	
■ 副 上海分行		1.北京分行	用户			北京分行		
🖻 📫 北京分行	Lawrence 1	起北京分行	安全组 - 通用			更多操作	11	•
	見行	起北京分行	通讯组 - 通用					
	#=	题北京分行	安全组 - 適用					
H 🛋 1	A	1.北南分行	安主地 · 西市 銀白					
🗷 🛋 i	AT	起北京分行	安全组 - 通用					
	7	84.北京分行	安全组 - 通用					
🗉 🛋 I	Ť -1	14. 北京分行	安全组 - 適用		-1			

在查看-自定义中可以选择用户可以在 UI 上进行的操作,选择好后确定。

屬 控制台1
文件 (F) 操作 (A) 查看 (V) 收藏夹 (0) 窗口 (W) 帮助 (H)
🗇 🔿 🚾 🥇 📋 添加/刪除列 (A) 🕐
大图标 (G)
□ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □
王 ■ 市场营销



自定义视图	\times
请选择或清除复选框来显示或隐藏控制台窗口的项目。	
✓ 标准菜单(操作和查看)@)	
▼ 标准工具栏(图)	
✓ 状态栏 (S)	120
□ 描述栏 @)	
☑ 任务板导航选项卡)	
☑ 操作窗格 (A)	
	_
□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□	
☑ 工具栏 Œ)	
	_

在文件-选项中,将控制台改名(可选),模式改为"用户模式-受限访问,单窗口"。勾选"不要保存对此控制台的更改",不勾选"允许用户自定义视图"。

🚟 控制台1			
文件() 操作(A)	查看(V) 收藏夹	(0) 窗口	
新建(N)	Ctrl+N	2	
打开(0)	Ctrl+0		
保存(S)	Ctrl+S		
另存为(A)			
添加/删除管理单元	(M) Ctrl+M	<u>称</u> 「中美村吉谷	
选项(P)		市场营销	
1 tsadmin		市场营销	
2 dsa		市场营销	
3 dinsmgmt		市场营销;	
4 dssite		市场宮钥 胡阳支行	
退出(X)		综合部	
		营业部	
□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□		行领导	
■ 🛛 🖃 🖬 财务管理	部 🔤 🚊	西城支行	
🔲 🗖 😂 Aitenii.	to ▼ 4		



选项
控制台 磁盘清理
▶ <u>北京</u> 00 更改图标 00
这些选项将在您下次打开 MMC 时生效。
控制台模式 (C):
用户模式 - 受限访问,单窗口
描述 在单一窗口模式打开管理单元控制台,阻止用户访问单一管理单 元控制台窗口看不见的树的区域。
 ✓ 不要保存对此控制台的更改 (S) □ 允许用户自定义视图 (V)

将自定义好的 mmc 保存后发给用户。并将 DC 上 system32 文件夹下的 adprop.dll、dsadmin.dll 和 dsprop.dll 拷贝到客户端的 system32 文件夹, 然后在客户端运行 regsvr32 adprop.dll、regsvr32 dsadmin.dll 和 regsvr32 dsprop.dll 注册这些文件。

然后在客户端上安装:

💽 Windows 功能	
打开或关闭 Windows 功能	
若要打开一种功能,请选择其复选框。若要关闭一种功能,请清除其复选 框。填充的框表示仅打开该功能的一部分。	
□→ 服务器管理器	
④ □ → 功能管理工具	
🗆 🔲 📄 角色管理工具	
⊛ 🔜 🤚 Active Directory 证书服务工具	
🖃 🔲 🔒 AD DS 和 AD LDS 工具	
🖃 📃 🔒 AD DS 工具	-
🔲] Active Directory 管理中心	6
🔲 🎍 AD DS 管理单元和命令行工具	~
	12.5
☑ ▲ AD LDS 管理单元和命令行工具	1
□ 用于 Windows PowerShell 的 Active Directory	· · ·
□ DHCP 服务器工具 🗸 🗸	
< •	
确定 取消	

这样客户端就可以管理特定 OU 而无法看到其它 OU 了。 注意:从 DC 上拷贝文件要和客户端对应,2008 R2 要拷到 Windows 7,且 32 位、64 位要 对应。



🚟 保存为		×
保存在(L):	三 桌面	💽 🕝 🌶 📂 🛄 -
夏 最近访问的位置	算 系统文件夹	admin2008 系统文件夹
桌面	は算机 系统文件夹	网络 系统文件夹
Ē Ē		
《 》 计算机		
网络	文件名(20): 北京の川	▼ 保存(S)
	保存类型(I): MS Management Console	文件 (*.msc) 🔽 取消

使用 BJDAG 登录 bj-dc01 后,将配置文档复制到域控上

	Lin ov
	BIDAG
rer	文档
	计算机
	网络



📸 北京OU						×
文件(F) 操作(A) 查看(V)	帮助(H)					
🖛 🔿 🖌 🗈 🏹 🧕	8 8 8	8 🖻 7 🖻	38			
1 北京分行 ○ ○ <th></th> <th>美型 组织织单位 组织织单位 组织织织单位 组织织织单单位 组织织织单单位 组织织单单位 组织织单单位 组织织单单位 组织织单单位 组织织单单位 组织织单单位 组织织单单位 组织织单单位</th> <th>描述</th> <th>Office Cor +</th> <th><mark>操作</mark> 北京分行 更多操作</th> <th>•</th>		美型 组织织单位 组织织单位 组织织织单位 组织织织单单位 组织织织单单位 组织织单单位 组织织单单位 组织织单单位 组织织单单位 组织织单单位 组织织单单位 组织织单单位 组织织单单位	描述	Office Cor +	<mark>操作</mark> 北京分行 更多操作	•
6	30555			i Shion	011	0



21

第3章 QA 3.1 暂无

