## Dayang Research Release





# Windows Server 2008 R2 SP1域策略 配置手册

文档信息:

Windows Server 2008 R2 SP1 域策略 配置手册			三册	
版本编号	版本日期	修改者	语言	更 新 说 明
V.1.0	2011-12-06	孙轶玮	中文	创建新文档

## 一、 版权说明

#### 关于本手册的版权归属

本技术文档所有权利归北京中科大洋科技发展股份有限公司所有。未经北京中科大洋科 技发展股份有限公司的书面许可,任何其他个人或组织均不得以任何形式将本文档的详细数 据和说明转载、复制、编辑或发布使用于其他任何场合;也不得把其中任何形式的资讯散发 给其他方。非本公司的,其他第三方不可把这些信息在其他的服务器或文档中作镜像复制或 保存。凡有意转载或使用本文档信息资料都属于违法行为,中科大洋科技发展有限公司有权 追究其法律责任。

北京中科大洋科技发展股份有限公司

## Windows Server 2008 R2 SP1 域策略 配置手册

## 目 录

—,	、 版权说明	
<u> </u>	背景描述	4
<u> </u>	功能描述	4
Ξ	配置前的准备	4
四	windows 2008 域控 安装配置	5
	4.1 安装操作系统	5
	4.2 配置网卡	5
	4.3 建立域控	
	4.4 配置辅助 DNS	
Ŧī.	部署域策略:	
	5.1 创建 OU 并新建用户和组	
	5.2 创建策略组:	
	5.3 设置登陆脚本	错误!未定义书签。
	5.4 重定向开始菜单	错误!未定义书签。
	5.5 管理模板策略	

#### 一 背景描述

在很多大洋项目具体实施中,都需要域策略的支持。基于 windows 2003 所部署的域策略,已经是大洋比较成熟稳定的域策略方案,如今,服务器操作系统已经升至 windows2008 平台,所以,我们迫切需要一套基于 windows2008 平台的域策略部署方案。本文主要介绍如何在 Windows Server 2008 R2 SP1 服务器进行一些常规域策略的部署,达到抛砖引玉的作用,帮助实施工程师根据项目具体需求,进行针对性的域策略的部署;

#### 二 功能描述

Windows Server 2008 R2 SP1 平台下的域策略,较 windows 2003 平台,有了更多完善的功能,在安全性方面,也得到了进一步得到了提高,通过本文档,我们可以实现如下一些安全域策略配置:

- 1. 基于网络驱动器域策略管理;
- 2. 基于应用程序域策略管理(重定向开始菜单);
- 3. 基于桌面隐藏等域策略管理;

#### 三 配置前的准备

#### a) 建立1-2台域控制器;

b) 安装操作系统: 安装下述任一版本均可
 Windows Server 2008 R2 SP1 标准版 64bit (安装时请选择完全安装)
 Windows Server 2008 R2 SP1 企业版 64bit (安装时请选择完全安装)

#### c) 关闭本机的防火墙:

注:加域前如果禁用防火墙,加域后需要再禁用一次,否则防火墙默认是被打开

### 四 windows 2008 域控 安装配置

#### 4.1 安装操作系统

安装 Win2008 R2 SP1 的方法此处不再赘述,但是对于此系统,操作系统在安装过程中 需要注意以下几点问题:

- 主机的硬件驱动识别正确
- 正确关闭防火墙

#### 4.2 配置网卡

对于网卡的 IP 地址划分如图:

Internet 协议版本 4(TCP/IPv4	)属性 ?×
常规	
如果网络支持此功能,则可以获取 您需要从网络系统管理员处获得适	自动指派的 IP 设置。否则, 当的 IP 设置。
○ 自动获得 IP 地址(0)	
┌ ⓒ 使用下面的 IP 地址(S):	
IP 地址(I):	192 .168 .200 .200
子网摘码(0):	255 . 255 . 255 . 0
默认网关 (0):	<u> </u>
C 自动获得 DNS 服务器地址 (B)	
└️ 使用下面的 DNS 服务器地址	(E):
首选 DNS 服务器 (P):	192 .168 .200 .200
备用 DNS 服务器(A):	192 .168 .200 .201
□ 退出时验证设置 (L)	高級(V)
	确定 取消

#### 其中涉及到的 IP 地址如下表:

主机	公网 IP	心跳 IP	虚拟 IP
主服务器	192.168.200.200/24	10.10.10.10/24	192.168.200.202/24
备服务器	192.168.200.201/24	10.10.10.11/24	192.168.200.202/24

#### 4.3 建立域控

建立域控时需要注意以下几点:

## 域控最好使用主备模式,即域控使用两台服务器来承担,一台为主域控,另一台 为从域控。

首先来建立主域控服务器,进入服务器管理器,点击左侧树状菜单中的角色按钮,在右面的窗口中点击"添加角色"按钮,如下图所示:

1. 服务器管理器		-0
文件(F) 操作(A) 查看(V) 表	8時 90	
💠 🔿 📶 🔝		
La 服务器管理器 (VIN-TVXP1LMVP)	角色	
	重看安装在服务器上角色的运行状况,以及类加或删除角色	5 NUDE -
	○角色編奏	■ 角色接要帮助
	◎角色: 己安装 0 个(共 17 个)	」。 「「「」」 「」」 「」」 「」」 「」」 「」」 「」」 「」」 「」」
	┃【3 上次朝鮮时间:今天 12:20 龍罴朝新	

在弹出的对话框中,选择"域服务",点击"下一步",如下图:

添加角色向导		×
选择服务器角色		
开始之前 服务器角色 Active Directory 域服务 确认 进度 结果	法経要安装在此服务器上的一个或多个角色。 角色(2):	描述: Active Directory J摄服务(AD_DS) 存除有关环路上对象的信息并使此 信息可用于用户和防管理员。AD DS 化使用煤空制器间中给用一段才通 过一个量变过程切问网络上任何所 术计资源的初限。

点击"下一步",如下图:

添加角色向导	x
Active Dir	rectory 域服务
开始之前 服务器角色 Active Directory 域服务 确认 进度 结果	Active Directory 妊娠外育介         Active Directory 妊娠外(10) ES)容结查天何強上的用户、计算机和EM设备价值是。AD ES 有助于管理交出管理支援意。并非助于用户间的演演重要和D.f.f. 自由自我的应用程序(例如 Microsoft Exchange Server)和其他 Yindows 服务器技术(例如相策略)也需要 AD ES         主要事例       • 蓋季百万         • 蓋季百万       • 重要有助的情况下用户仍然可以登录到网络,请至少为域安装两个域空制         • 加 ES 要求将 DDS 服务器安装在网络上。如果未安装 DDS, 系统会提示您在该服务器上安装 DDS 服务器角色。         • 記念 要求将 DDS 服务器安装在网络上。如果未安装 DDS, 系统会提示您在该服务器上安装 DDS 服务器通合。         • 支张 AD IS 之后,使用 Active Directory 技服务安装同号 (acprono.exe)使服务器成为全功能域 控制器。         • 支张 AD IS 将在属句明安装自录服务所需的 DFS 命名空间、DFS 重制和文件复制服务。         其他信息         AD IS 都述         变法 AD ES         AD IS 新游
	< 上一步 Q) │ 下一步 Q0 > 」 安裝 CD │ 取消

点击"安装",如下图:

添加角色向导	×
确认安装选择	
开始之前 服务器角色 Active Directory 域服务 通过 进度 结果	<ul> <li>着要安装以下角色、角色服务或功能,请单击"安装"。</li> <li>① 2 条提示性消息显示如下</li> <li>④ 安装完成之后,可能需要重新启动该服务器。</li> <li>● Active Directory 域服务</li> <li>● Active Directory 域服务安装向导(deprono. exe)使服务器成为全 功能/域控制器。</li> </ul>
	打印。保存或通过电子邮件发送此信息
	< 上一步 @ ) 下一步 @ ) ( 安装 @ ) 取消

开始进行角色的安装,如下图:

添加角色向导	
安装进度	
开始之前	正在安装以下角色、角色服务或功能:
服务器角色	Active Directory 域服务
Active Directory 取服穷 确认	
进度	
结果	
	< <li>(上一步 (2)) 下一步 (2) / 安装 (2) 取消</li>

在安装结束后回弹出如下对话框,点击红色框图圈中的连接,窗口会自动关闭,进入到

配置阶段,如下图:

添加角色向导	X
安装结果	
开始之前 服务器角色 Active Directory 域服务 确认 进度 <b>结果</b>	<ul> <li>□ 民助安装以下角色、角色服务或功能:         <ul> <li>▲ 名爾男 : 希提示性清電显示如下</li> <li>▲ 和田 Windows 自动更新。为确保自动更新最新安装的角色或功能。请自用"控制面板"中 10 Windows Updates</li> <li>▲ Active Directory <b>试服务</b></li> <li>④ 安装成功</li> <li>□ 合果实以下角色服务:</li> <li>▲ Comparison of the Directory <b>试服</b>务安装向导 (depromo.exe) 使该服务器成为完全正常运行的域 交易的导并启动 Active Directory <b>域服</b>务安装向导 (depromo.exe) (</li> </ul> </li> </ul>
	打印、保存或通过电子邮件发送支装报告
	<上歩む)下歩図>) <b>美闭@</b> 取消

下面开始对域控服务进行配置,此操作在主域控服务器上进行

勾选"使用高级模式安装",点击"下一步",如下图:



保持默认,点击"下一步",如下图:

and Active Directory 域服务安装向导	×
操作系统兼容性 Windows Server 2008 和 Windows Server 2008 R2 中改进的安全设置影 响旧版 Windows	
<ul> <li>Windows Server 2008 和 Windows Server 2008 N2 域控制器为名为"允许与 Windows NT 4.0 兼容的加密算法"的安全设置提供了更安全的新默认值。此设置可防止 Wirdows Server 2008 和 Windows Server 2008 式 域控制器建立安全通道会话时使用较弱的 NT 4.0 类型加密算法。此新默认值可能导致需要用 Windows Server 2008 成 Windows Server 2008 NZ 域控制器提供安全通道的操作或应用程序失败。</li> <li>受此更改影响的平台包括 Windows NT 4.0 及非 Microsoft SMB "客户端" 和不支持税经通加密算法的网络附加存储 (MAS)设备。在运行 Windows Vista Service Pack 1 以前版本的 Windows 客户端上的部分操作也会受到影响。 包括由 Active Directory 迁移工具或 Windows 部署服务执行的域加入操作。</li> <li>有关此设置的更多信息,请参阅知识库文章 942564 (http://go.microsoft.com/fwlink/?LinkId=104751)。)</li> </ul>	
<上一步(B) 下一步(D) > 取消	

选择"在新林中新建域",点击"下一步",如下图:

on Active Directory 域服务安装向导	×
<b>选择某一部署配置</b> 您可为现有林或新林创建域控制器。	
◎ 现有林 健)	
C 向现有域添加域控制器 (A)	
○ 在现有林中新建域 C) 此服务器将成为新域中的第一个域控制器。	
■ 新建域树根而不是新子域(II)	
<ul> <li>○ 在新林中新建域 (D)</li> </ul>	
有关可能的部署配置的详细信息	
〈上一步 03)下一步 07) 〉	取消

在输入框中输入域名称,此处输入的是"dayang.com",点击"下一步",如下图:

on Active Directory 域服务安装向导	×
<b>命名林根域</b> 林中的第一个域是林根域。其名称也是该林的名称。	
键入新目录林根级域的完全限定的域名 (FQDN)。	
目录林根级域的 FQDN (F):	
dayang.com	
例切: corp.contoso.com	
〈上一步 (3) 下	步 08) > 取消

如下图:点击"下一步"

a Active Directory 域服务安装向导	×
<b>域 WetBIOS 名称</b> 这是 Windows 早期版本的用户用于标识新域的名称。	
此向导生成一个默认的 NetBIOS 名称。只有在您已选择了高级模式或此向导已检测到与默认名称的冲突时才会显示此向导页。 按照向导生或的名称,或考键)新名称。然后第五"下一步"。	
这天间守工城印石柳,纵目雄八孙石柳,公石千山 下于罗 。	
域 NetBIOS 名称(D): DAYANG	
< 上一步 (8) 下一步 (8) ▶ 取	消

在"林功能级别"选项中选择"Win2008 R2",点击"下一步"如下图:

选择林功	<del>×27</del> 能級别。	
林功能级; Windows	別(F): Server 2008 R2	T
详细信息 Windows 级别中可 S 默认情况 功能级别	D): Server 2008 B2 林功能级别提供 Windows 用的所有功能,以及以下附加功能: 回收站,启用后,它提供运行 Active Dire 完整还更删除的对象的功能。 下,在该林中创建的任何新域将在 Windows 下操作。	Server 2008 林功能 🔺 actory 域服务时 Server 2008 R2 域
<u>个</u> 有关 <u>域和</u>	您将只能向该林添加运行 Windows Server 本的域控制器。 <u>木功能级别</u> 的详细信息	2008 № 或更高版

勾选"DNS 服务器",点击"下一步"

ctive Directory 虞振为女装问寻	
其他域控制器选项	
为此域控制器选择其他选项。 ✔ DNS 服务器 (D)	
▶ 王向明末(v) ▶ 只读域控制器(RODC)(R) 其他信息(A):	
林中的第一个域控制器必须是全局编录服务器且不能是 RODC。 建议您将 DNS 服务器服务安装在第一个域控制器上。	<u> </u>
	Ţ

在弹出的对话框中,选择"是"选项,

<b>司</b> 静态	s IP 分配 🛛 🕅
Û	此计算机具有动态分配的 IP 地址
	此计算机上至少有一个物理网络适配器未将静态 IP 地址分配给其 IP 属 性。如果同时为某个网络适配器目用 IFV4 和 IFV6,则应将 IFV4 和 IFV6 静态 IP 地址分配给该物理网络适配器的 IFV4 和 IFV6 属性。应 对所有物理网络适配器执行此类静态 IP 地址分配,以便执行可攀的域名 系统 UNS)操作。 是否要在未分配静态 IP 地址的情况下继续执行操作?
	→ 是(T),该计算机将使用 DHCP 服务器自动分配的 IP 地址( 不推荐)。
	→ 否(II),将静态 IP 地址分配给所有物理网络适配器。
1	

如下图,点击"是"



保持默认,点击"下一步"如下图:

on Active Directory 域服务安装向导	×
<b>数据库、日志文件和 STSVOL 的位置</b> 指定将包含 Active Directory 域控制器数据库、日志文件和 SYSVOL 的 文件夹。	
为获得更好的性能和可恢复性,请将数据库和日志文件存储在不同的卷上。	
数据库文件夹 (0):	
<mark>E:\Windows\NTDS</mark> 浏览(R)	
日志文件文件夹 (L):	
C:\Windows\MTDS 浏览(0)	
SYSVOL 文件夹 (S):	
C:\Windows\SYSVOL 浏览(W)	
有关 <u>放器 Active Directory 域服务文件</u> 的详细信息	
〈上一步 (8) 下一步 (87) 〉 取消	

为目录服务还原模式的 Administrator 设置一个新密码,如下图:

■ Active Directory 域服务安装向导	×
目录服务还原模式的 Administrator 密码	
目录服务还原模式 Administrator 帐户不同于域 Administrator 帐户。	
为 Administrator 帐户分配一个密码,将在以目录服务还原模式启动此域 制器时使用该帐户。我们建议您选择一个强密码。	Ŷ
密码 健): ●●●●●●●	
确认密码 (C): ●●●●●●●	
关于目录服务还原模式密码的详细信息	
< 上一步 (8) 下一步 (0) >	取消

保持默认,点击"下一步"

on Active Directory 域服务安装向导	×
摘要	
检查您的选择 (R): 将该服务器配置为新林中的第一个 Active Directory 域控制器。 新域名为"dayang.com"。这也是新林的名称。 域的 NetBIOS 名称为"DAYANG"。 林功能级别: Windows Server 2008 R2 域功能级别: Windows Server 2008 R2 站点: Default-First-Site-Name 其他选项:	
要更改选项,单击"上一步"。要开始操作,单击"下一步"。 可以将这些设置导出到一个应答文件中以用于其他无人 参与操作。 有关 <u>使用应答文件</u> 的详细信息	J
〈上一步(8) 下一步(01) 〉 取	消

系统开始配置域控

Active Directory 填服务安装向导
向导正在配置 Active Directory 域服务。此过程可能需要几分钟到几小时, 具体依您所选的环境和选项而定。
正在安装组策略管理控制台

域控服务配置完成之后,系统会重新启动。

**下面开始配置备用域控,以下操作在备服务器上操作:** 安装域控角色的步骤与前面一样,下面介绍配置备用域控的方法: 如下图:选择"向现有域添加域控制器",点击"下一步"

od Active Directory 域服务安装向导	×
<b>选择某一部署程置</b> 您可为现有林或新林创建域控制器。	
<ul> <li>现有林(E)</li> <li>向现有域添加域控制器(A)</li> <li>在现有林中新建域(C) 此服务器将成为新域中的第一个域控制器。</li> <li>新建域树根而不是新子域(E)</li> <li>C 在新林中新建域(D)</li> </ul>	
有关可能的部署配置的详细信息 <u>〈上一步</u> (B) 下一步	(N) > 取消

在输入栏中添加域的名称,前面建立域的名称是"dayang.com"这里也输入相应的名称,如下图:点击使用"备用凭据",输入域管理员的用户名密码,点击"下一步"

■ Active Directory 域服务安装向导 X
<b>网络凭据</b> 指定将在其上执行安装的林的名称,以及具有执行安装所需的足够权限的 帐户凭据。
键入位于计划安装此域控制器的林中任何域的名称(IT):
请指定用于执行安装的帐户凭据:
○ 我的当前登录凭据(MSCS-2\Administrator)(C) 因为当前用户凭据是该计算机的本地凭据,所以无法选择。需要一组减凭
○ 备用凭据(A):
dayang.com\Administrator
有关谁可以安装 Active Directory 域服务的详细信息
< 上一步 (B) 下一步 (M) > 取消

系统找到域,点击"下一步",如下图:

active Directory 域服务安装向导	
5.择域	
为该额外域控制器选择域。	
域(0):	

保持默认,如下图,点击"下一步"

★#一丁始息 为新域控制器选择一个站点。 ■ 使用与此计算机的 IP 地址对应的站点 00)。 站点 (S):	医#一丁始島       为新域控制器选择一个站点。       ■       使用与此计算机的 IP 地址对应的站点 00)。       站点 (S):       」	* 17 ልት ድ		ſ
■ 使用与此计算机的 IP 地址对应的站点 UD。 站点 (S): Default-First-Site-Name	■ 使用与此计算机的 IP 地址对应的站点 UD 。          站点 (S):         站点       描述         Default-First-Site-Name	为新域控制器选择一个站点。		
站点(S): 站点    描述	站点(S): 站点 描述 Default-First-Site-Name	┏ 使用与此计算机的 IP 地址	L对应的站点(V)。	
站点 描述 Default-First-Site-Name	站点 描述 Default-First-Site-Name	站点(S):		
Default-First-Site-Name	Default-First-Site-Name	站点	描述	

保持默认,如下图,点击"下一步"

on Active Directory 域服务安装向导	×
其他域控制器选项	
为此域控制器选择其他选项。	
▼ DNS 服务器 (0)	
✓ 全局编录(G)	
□ 只读域控制器 (RODC) (R)	
其他信息 (A):	
当前存在一个注册为该域的权威性名称服务器的 DMS 服务器。	
有关 <u>其他域控制器选项</u> 的详细信息	
< 上一步 (B) 下一步 (N) > 取消	

如下图:选择"是"

<b>司</b> 静态	s IP 分配 🛛 🛛
	此计算机具有动态分配的 IP 地址
	此计算机上至少有一个物理网络适配器未将静态 IP 地址分配给其 IP 属 性。如果同时为某个网络适配器启用 IPv4 和 IPv6,则应将 IPv4 和 IPv6 静态 IP 地址分配给该初望网络适配器的 IPv4 和 IPv6 属性。应 对所有物理网络适配器执行此类静态 IP 地址分配,以便执行可靠的域名 系统 URX)操作。 是否要在未分配静态 IP 地址的情况下继续执行操作?
	→ 是(T),该计算机将使用 DHCP 服务器自动分配的 IP 地址( 不推荐)。
	→ 否(B),将静态 IP 地址分配给所有物理网络适配器。
() ž	

如下图:选择"是"



保持默认,如下图:点击"下一步"

■ Active Directory 域服务安装向导 ×
从介质安装
根据您是希望通过网络复制现有域控制器的域数据,还是希望通过创建的媒体复制现有域控制器的域数据(从媒体安装),选择以下选项之一。在任何一种情况下,现有域控制器都必须与新的域控制器位于同一个域中。
<ul> <li>通过网络从现有域控制器复制数据(0)</li> <li>从下列位置的介质中复制数据</li> <li>查阅帮助以确保所使用的媒体与所安装的域控制器的类型兼容。即使选择了此选项,某些数据仍会通过网络复制。</li> </ul>
位置 (L): C:\NTDSRestore 必须已从可写域控制器中而不是只读域控制器中创建了您所选的媒体。 有关 <u>从媒体安装</u> 的详细信息
<上一步 (B) 下一步 (M) > 取消

保持默认,如下图:点击"下一步"

Active Directory 域服务安装向导	×
<b>湏</b> 嫧控制器	
可让向导为该域控制器的安装选择一个复 控制器。即使您选择从媒体安装,也必须 某些数据与入此复制伙伴。	制伙伴,或者可指定一个要使用的域 从该复制伙伴复制某些数据,并且将
为安装伙伴选择源域控制器: ● 让向导选择一个合适的域控制器 Œ) ● 使用此特定的域控制器 颐):	
域控制器名称	站点名称
MSCS-1. dayang.com	Default-First-Sit
有关法择安装合作伙伴的详细信息	
	(上一步(B) [トー步(A) > _ 取消

保持默认,如下图:点击"下一步"

Nactive Directory 域服务安装向导 🛛 🗙 🗙			
<b>数据库、日志文件和 STSVOL 的位置</b> 指定将包含 Active Directory 域控制器数据库、日志文件和 STSVOL 的 文件夹。			
为获得更好的性能和可恢复性,请将数据库和日志文件存储在不同的卷上。			
数据库文件夹 (0):			
C:\Windows\NTDS			
C:\Windows\NTDS 浏览(0)			
SYSVOL 文件夹 (S):			
C:\Windows\SYSVOL 浏览(W)			
有关 <u>`` Active Directory 域服务文件</u> 的详细信息			
〈上一步 (8) 下一步 (87) 〉 取消			

输入一个新密码,如下图,点击"下一步"

a Active Directory 域服务安装向导	×
目录服务还原模式的 Administrator 密码	
目录服务还原模式 Administrator 帐户不同于域 Administrator 帐户。	
为 Administrator 帐户分配一个密码,将在以目录服务还原模式启动此域控制器时使用该帐户。我们建议您选择一个强密码。	
密码 (0): ●●●●●●●	
确认密码 (C):	
关于目录服务还原模式密码的详细信息	
〈上一步 (8) 下一步 (8) 〉 取消	

保持默认,如下图,点击"下一步"

active Directory 這服务安装向导	
	4
检查您的选择 (R): 将该服务器配置为域"dayang.com"的附加 Active Directory 域控制器 。 	-
NAL: Default=First=Site=Rame 其他洗顶: 只读域控制器:"否" 全局编录:是 DNS 服务器:是	
更新 DNS 委派: 否 源域控制器: 任何可写入的域控制器	•
要更改选项,单击"上一步"。要开始操作,单击"下一步"。	
可以将这些设置导出到一个应答文件中以用于其他无人 参与操作。 有关使用应答文件的详细信息	

勾选"完成后重新启动",系统在配置完成之后会自动重启服务器的操作系统

Active Directory 域服务安装向导
向导正在配置 Active Directory 域服务。此过程可能需要几分钟到几小时, 具体依您所选的环境和选项而定。
等待 DNS 安装完成
取消 「○ 完成后重新启动 (8)

到此, 主备域控的配置就完成了。

#### 4.4 配置辅助 DNS

在建立完成主备域控之后,我们需要对两台 DNS 服务器进行 DNS 记录的自动同步的配置,具体方法如下:

首先在第二台服务器,即备域控服务器上点击"开始---管理工具---DNS",在根节点即 机器名上点击鼠标右键,选择"属性",出现如下对话框,选择"转发器"页签,点击"编 辑"按钮,添加主域控的 IP 地址,等待系统进行网络扫描。

完成之后,点击确定,退出。

Dayang Research

ISCS-2 属性	? ×
事件日志         信任定位点         监视           接口         转发器         高级         相提示	安全   调试日志
转发器是可以用来进行DNS记录查询的服务器,而这些 器无法解决的。	纪录是该服务
IP 地址 服务器 FODN	
192.168.200.200 MSCS-1	
🔽 如果没有转发器可用,请使用根提示	编辑(E)
注意:如果为给定域定义了条件转发器,则将使用它们 级别的转发器。若要创建或查看条件转发器,请浏览到 条件转发器节点。	门代替服务器 则范围树中的
确定 取消 应用 (A)	帮助

此时就完成了辅助 DNS 的配置,为了验证配置生效,我们登陆到第一台服务器上,按照上述方法,打开主 DNS 的"转发器"页签,可以看到如下图:

在未进行配置的情况下,主 DNS 服务自动进行了识别,可以看到窗口中已经有 MSCS-2 的机器在,说明辅助 DNS 配置成功。

ISCS-1 属性	? ×
事件日志         信任定位点         监视           接口         转发器         高级         根提示           转发器是可以用来进行DMS记录查询的服务器,而这些	安全   调试日志   纪录是该服务
器无法解决的。 TP 地址 服务哭 FOIN	
192.168.200.201 MSCS-2	
□ 如果没有转发器可用,请使用根提示	编辑(2)
注意: 如果为给定域定义了条件转发器,则将使用它们 级别的转发器。若要创建或宣看条件转发器,请浏览到 条件转发器节点。	门代替服务器 到范围树中的
	帮助

#### 五 部署域策略:

在完成了域控与 DNS 的主备系统部署之后,我们开始在主域控上进行域的部署。为了顺利 完成配置任务,我们需要在配置之前验证下面的准备工作是否已经完成并没有出现报错:

#### ● 防火墙已经关闭。

使用 windows 2008 R2 域策略,可以实现所有站点有统一的界面;可以使用户没有任何 设置涉及系统安全性方面的权力,所有对安全性的设置大部分都在服务器端只设置一次,只 有很少量的设置需要在各客户端设置,接下来,开始介绍如何安装部署域策略功能:

#### 5.1 创建 OU 并新建用户和组



其中, dayangtv 是 OU, 即一个域中的组织单位, edit 是一个用户, 即在客户端登陆 windows 2008 R2 的用户名, dayangedit 是一个全局安全组, 具体创建过程如下:

开始一所有程序一管理工具-Active Directory 用户和计算机,展开左边树,如图所示:

📔 Active Directory 用户和计算机			
文件()F) 操作(A) 查看(V) 帮助(H)			
(= =) 🖄 🖬 📋 🖬 🙆 🛃	] 🖬 🗏 🐮 👕 🖓 🕯	2 <sup>3</sup> 8	
▲ Active Directory 用户和计算机       名称         ●       保存的查询         ●       ●	类型       niltin     builtinDoma:       mputers     容器       nain Co     组织单位       reignSe     容器       naged S     容器       ers     容器       ers     容器       ers     行器       ers     行器	描述 In Default container fo Default container fo Default container fo Default container fo Default container fo	
<ul> <li>Ⅲ Ⅲ Ⅲ Ⅲ ↓</li> <li>Ⅲ Ⅲ Ⅲ ↓</li> <li>Ⅲ Ⅲ Ⅲ ↓</li> <li>Ⅲ Ⅲ Ⅲ ↓</li> <li>Ⅲ ↓</li></ul>	it算机 联系人 组 InetOrgPerson msImagingTSPs MSMQ 队列别名 组织单位 打印机 用户		
	**		

选中 test.com 右键-新建-组织单位,如下图:

新建对象 - 组织单位	×
🧭 创建于: test.com/	
名称(4):	
dayangtv	
▶ 防止容器被意外删除 ℓ)	
	-
确定 取消 帮助	

输入组织单位名称: dayangtv,确定,创建 OU 结束。

然后在 OU 上创建组,在 dayangtv-右键-新建-组,如下图

新建对象 - 组		×
総理子: test.com/da	ayangtv	
组名(4):		
dayangedi t		
组名(Windows 2000 以前版本)(	<i>"</i> ):	
dayangedit	-	
─ 组作用域 ─────		
○ 本地域 (0)	● 安全组 (S)	
<ul> <li>● 全局 (G)</li> </ul>	○ 通讯组 @)	
○通用Ψ		
	确定 取消	á l

输入组名: dayangedit, 组作用域: 全局, 组类型: 安全式, 确定, 创建组完成。 同样, 创建用户, 在 dayangtv-右键-新建-用户, 如下图:

新建对象 - 用户		×
🧏 创建于:	test.com/dayangtv	
姓 (L):	edit	
名(2):	英文缩写 (I):	
姓名(A):	edit	
用户登录名(U):		
edi t	@test.com 💌	
用户登录名(Window	vs 2000 以前版本)(ሢ):	
TEST\	edit	
	<上一步(B) 下一步(B) > 取消	Í

输入需要创建的用户名登陆名: edit, 姓名: edit, 点击下一步:

新建对象 - 用户	×
🔏 创建于: test.com/dayangtv	
密码 (E): 确认密码 (C): ●●●●●	
- □ 用户下次登录时须更改密码 @) ■ 用户不能更改密码 ©)	
✓ 密码永不过期 (2) ► 帐户已禁用 (2)	
<上一步(B) 下一步(D) > 取消	í

输入密码,并选中:用户不能更改密码;密码永不过期,点击下一步:

新建对象 - 用户	×
🔏 创建于: test.com/dayangtv	
您单击"完成"后,下列对象将被创建:	
全名: edit	<b>A</b>
用户登录名: edit@test.com	
用户不能更改密码。 密码永不过期。	
	<b>T</b>
< 上一步 (B) [[]] 完成 []	取消

创建完成,点击确定。

然后修改用户属性,使其加入到 edit 组中,在新建的用户名上右键-属性-隶属于-添加-

选中 dayangedit 一添加,这样把用户添加到 dayangedit 全局安全组。

若需要建立其它帐号,可依上样建立,如 edit1、edit2、edit3 三个用户。

Dayang Research

#### 5.2 创建策略组:

组策略使用来设置 windows 登陆安全的策略,比如屏蔽客户端左面右键,开始菜单,资源管理器等,组策略针对 OU,所有设置只涉及"用户配置"中的"windows 设置"和"管理模板"。



开始-所有程序-管理工具-组策略管理,展开左边树,如图所示:

■ 組策略管理	
🔜 文件 (F) 操作 (A) 查看 (Y) 窗口 (H) 帮助 (H)	
🗢 🔿 📂 🖬 📋 💥 🖾 🧟 🔽 🖬	
<ul> <li>紅策略管理</li> <li>▲ 新: test.com</li> <li>● 載 test.com</li> <li>● Default Domain Policy</li> <li>● Default Domain Controllers</li> <li>● 如果範別象</li> <li>● Default Domain Controllers Policy</li> <li>● Default Domain Policy</li> <li>● Unit With With With With With With With Wi</li></ul>	dayangtv         链接的组第略对数       组策略继承       要派

右键,选择在这个域中创建 GPO 并在此处链接:



Dayang Research

第 27 页 总 34 页

弹出的对话框中"新建 GPO"中,输入 tvconfig,建立策略组,点击确定;

新建 GPO	×
名称 (2):	
tvconfig	
源 Starter GPO(S):	
(先)	•
	 取消

选甲 tvconfig, 右键选择编辑, 如下图	选中 tvconfig,	右键选择编辑,	如下睯	٤l:
--------------------------	--------------	---------	-----	-----

<u>属</u> 组策略管理	
🔜 文件 (F) 操作 (A) 查看 (V) 窗口 (W) 帮助 (H)	
🗇 🔿 🗾 🗰 🔀 🖬 🖬	
▲ 组第略管理 → 从 林: test.com → 」「」 → 「」」 → 「」」」 → 「」」 → 「」」 → 「」」 → 「」」 → 「」」 → 「」」 → 「」」」 → 「」」 → 「」 → 「」」 → 「」 → 「 → 「 → 「 → 「 → 「 → 「 → 「 → 「	tvconfig 作用域  详细信息  设置   委派   磁技 在此位置内显示链接 ①: test.com 下列站点、域和组织单位链接到此 GPO (T): 位置 ▲
	安全筛选 (# GPD 内的沿景中应用于下沟(组、用户和计算机 (5)·
	Authenticated Users

<b>」</b>			_ 🗆 🗡
文件 (P) 操作 (A) 查看 (V) 帮	)助(H)		
🗢 🄿 🗖 🖬 📓 🛃 🖬			
圓 tvconfig [WIN-R250PJK9T2C.TF □ № 计算机配置	🗐 tweenfig [WIN-R250PJK9T20	C.TEST.COM] 策略	
		名称	
■ 🗉 🛄 首选项		▶️计算机配置 ┛ 田 白雨)罢	
		1995 用尸郎五	
🛛 🖸 首选项			
	\扩展/标准/		
]			

在弹出的组策略管理编辑中,根据项目要求,进行相应编辑

## 六 域策略具体应用场景:

#### 6.1 基于网络驱动器域策略管理

点"编辑"该组策略对象链接名,策略组一用户配置一windows设置一脚本(登陆/注销),如

下图:

🧾 组策略管理编辑器			
文件 (27) 操作 (A) 查看 (V) 帮	助田		
🗢 🔿 🔰 📅 🖬 🗟 👔	) E		
tvconfig [WIN-R250PJK9T2C. TE	副 脚本(登录/注销)		
□ 🐏 计算机配置			
□ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □	登录	_ <del>  </del> 裕禄 	
日 🕵 用户配置	显示 <u>属性</u>	a 注销	
□ □ □ 泉崎 ⊡ □ □ \$\$	┃ 描述:		
드 🦳 Windows 设置	数据包含用户登录脚本。		
□ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □			
□ 🚞 文件夹重定向			
王 📶 基丁策略的 QoS 王 🕷 Internet Explor			
🗉 🧰 管理模板: 从本地计:			
④ 🖸 🛄 首选项			
	\11 . 172 / (11/) / (1		

双击登录,如	山下图	:
--------	-----	---

登录 属性	?×	
脚本 PowerShell 脚本		
登录 脚本(tvconfig 的)		
名称    参数	上移 (1) 下移 (1)	
	<b>添加 @</b> 编辑 @	
	刪除 (2)	
要查看保存在此组策略对象中的脚本文件,请按下面按钮。 显示文件 (S)		
确定 取消	应用 (A)	

点击显示文件,将展开浏览器,然后在该文件夹中新建登陆脚本文件(登陆脚本针对磁盘阵

列的盘符映射),如下例:



将该文件保存为 disk.bat,这样用户登陆时在本地工作站映射共享盘符。

然后在登录属性中点击添加一浏览一选中disk .bat一确定,这样就配置完成了用户登陆脚本。

#### 6.2 基于应用程序域策略管理(重定向开始菜单):

策略组一用户配置-windows设置-文件夹重定向-[开始]菜单-属性,如下图:



「开始」菜单 属性	<u>? ×</u>
目标   设置	
可以指定 「开始」 菜单 文件夹的位置。	
设置 (S): 基本 - 将每个人的文件夹重定向到同一个位置	•
该文件夹会被重新定向到指定的位置。	
_ 目标文件夹位置 (I)	
重定向到下列位置	]   [
根路径 @):	_
C:\Users\Administrator\Documents\程序组	
[浏览 B)	
	(A)

配置说明:我们将目标文件夹设置为: C:\Users\Administrator\Documents\程序组,这样我们 需要在每个工作站上用 administrator 登陆后,在C盘我的文档中建立文件夹"程序组",把 我们需要的软件快捷方式如: Xedit, Newsmanage 拷贝到该文件夹,这样,用户登陆后在开 始菜单中只出现我们需要的快捷方式。注意:在设置该项后,要在所有站点上以某个 edit 组用户登录,然后删除系统在程序组中自动生成的快捷方式。

#### 6.2 基于桌面隐藏等域策略管理:

管理模板策略主要是用来屏蔽桌面等设置,在组策略一用户配置一管理模板中,对相应的策略设置启用。

1. 桌面的设置(位置在"管理模板"→"桌面")

- 1) 启用"隐藏桌面上的所有图标"
- 2) 启用"禁止添加、托、放和关闭任务栏的工具栏"
- 3) 启用"禁用调整着桌面工具栏"
- 2. 任务栏和开始菜单的设置(位置在"管理模板"→"任务栏和开始菜单")
- 1) 启用"从开始菜单上删除'文档'菜单"
- 2) 启用"从开始菜单中删除'搜索'菜单"
- 3) 启用"从开始菜单中删除'收藏夹'菜单"
- 4) 启用"从开始菜单中删除'运行'菜单"
- 5) 启用"从开始菜单删除'帮助'命令"(可选)
- 6) 启用"从开始菜单删除'网络和拨号连接'"(可选)
- 7) 启用"禁用并删除'Windows Update'的链接"
- 8) 启用"禁用开始菜单上的拖放上下文菜单"
- 9) 启用"在设置菜单上禁用程序"
- 10) 启用"将'注销'添加到开始菜单"(可选)
- 11) 启用"禁止更改'任务栏和开始菜单'设置"
- 12) 启用"禁用任务栏的上下文菜单"注:在设置该项前,要在所有站点上以该用户登录, 然后在任务栏右击,在"工具栏"中取消"快速启动"。(这样可以更加提高安全性,但 此项设置也可以做为可选项)本项设置最好删除程序组里自动生成的快捷方式,这样可 以减少工作量。
- 13) 启用"从开始菜单删除公用程序组"
- 3. 限制用户网络设置权限(在"管理模板"→"网络"→"网络及拨号连接")
- 1) 启用"禁止启用/停用 LAN 连接"
- 2) 启用"禁止访问 LAN 连接的属性"

最后在工作站本地登录,并在本地 Administrators 组中添加 test.com/edit 这个组,这样做可 以使登陆用户仅能使用 edit 用户所配置的权限。 这样网络权限安全性设置完成。