Windows 域控管理

说明：

1.本文档没有目录，本文档在发布时为 pdf 文档，有章节书签，可以下载到本地来查看，点击书签进入相应的章节。

2.蓝色的字为配置命令，绿色的字为命令的注释，有时命令太密集时，就不用蓝色标出了。

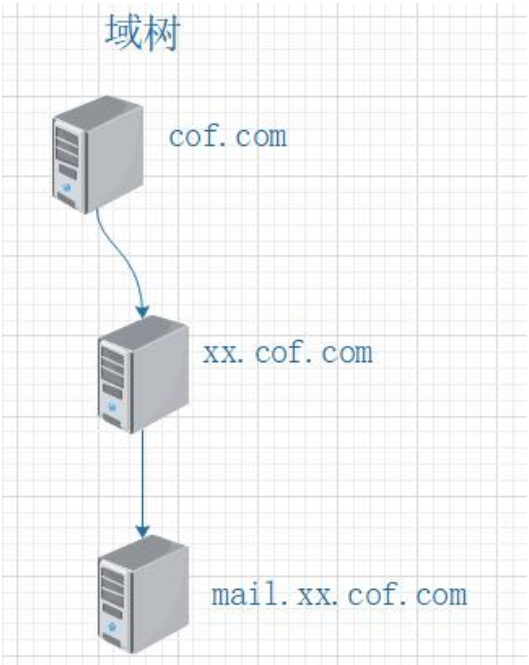
3.注意：本文档的所有操作请先在在虚拟机里进行实践，请不要直接在真实的服务器中操作！

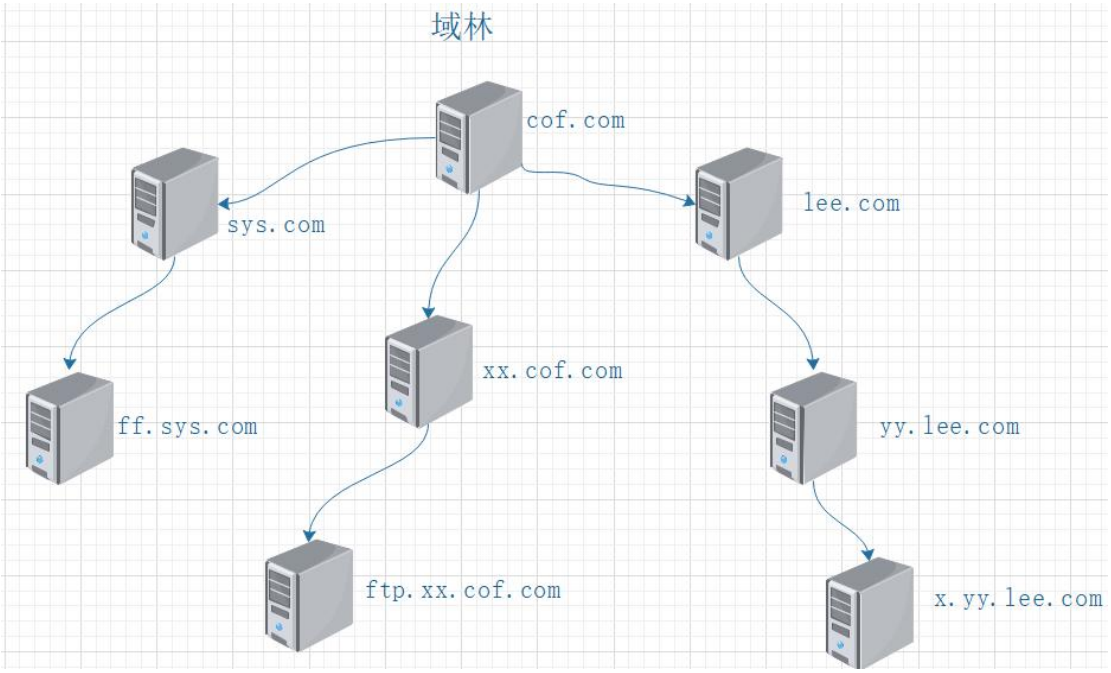
作者：李茂福

日期：2019 年 12 月 24 日

Windows 域

Windows 中的 域（domain）是一套统一的身份验证系统，是企业应用的基础。组策略通过用户身份验证 和域绑定得比较紧密。





域树：由多个域组成，这些域共享同一个存储结构和配置，形成一个连续的名字空间，有相同的 DNS 后缀。

域林：由一个或多个没有形成连续名字空间的域树组成，构成域林的各个域树之间没有形成连续的名字空间，没有相同的 DNS 后缀。但域林中的所有域树仍共享同一个存储结构、配置和全局目录。

根域：网络中创建的第一个域，一个域林中只能有一个根域（Root Domain）。

DC > get-ADforest　　//查看根域

部署第一台域控制器

1.以管理员帐号 Administrator 登录服务器
2.更改计算机名
3.设置静态 IP
4.首选 DNS 配置为本机 IP
5.添加角色和功能：
打开“服务器管理器”→添加角色和功能→基于角色或基于功能的安装→...→Active Directory 域服务→....→安装进度（结果）→点击“将此服务器提升为域控制器→添加新林
一般第一台域控制器同时也是“集成区域 DNS 服务器”

>net　accounts　　//查看计算机角色，第一台域控的角色为 Primary
>net　share　　//查看系统共享卷，以下为安装 DC 功能后添加的
NETLOGON　C:\Windows\SYSVOL\sysvol\guotai.com\SCRIPTS　Logon server share
SYSVOL　C:\Windows\SYSVOL\sysvol　Logon server share

FSMO 操作主机角色

Flexible Single Master Operation

>netdom query fsmo //查看 5 种操作主机角色所在的域控制器

1.架构主机 Schema Master

域林中只有一个架构主机，作用是定义所有域的对象属性（定义数据库字段及存储方式）

2.域命名主机 Domain Naming Master

域林中只有一个域命名主机，负责控制域林内域的添加或删除

3.PDC 主机 PDC Emulator Master

每个域中只有一个 PDC 主机，作用：

兼容低版本的 DC

PDC 主机角色所在的 DC 优先成为主域浏览器，用>net accounts 查看的那个 Primary

活动目录数据库的优先复制权

时间同步

防止重复套用组策略，使用组策略时，组策略编辑器默认连到 PDC 主机

4.RID 主机 Relative Identifier Master

每个域中只有一个 RID 主机

作用是 在域中创建对象时保证每个对象有一个唯一的 SID，跨域访问、迁移域对象时，通过 RID 主机确认域对象的唯一性

5.基础结构主机 Infrastructure Master

每个域中只有一个基础结构主机，负责对跨域对象的引用进行更新

*整个域林中只有一台架构主机和一台域命名主机

*每个域中都有自己的 PDC 主机、RID 主机和基础架构主机 各一台

FSMO 角色转移

将 Primary 上的操作主机角色转移到 Backup 上

登录 Backup DC

>ntdsutil

ntdsutil: roles

Fsmo maintenance: connections

Server connections: connect to server BackDC.cof.com //连接至 Backup DC

server connections: quit

Fsmo maintenance: transfer schema master //转移架构主机角色

Fsmo maintenance: transfer naming master //转移域命名主机角色

Fsmo maintenance: transfer RID master //转移 RID 主机角色
Fsmo maintenance: transfer PDC //转移 PDC 主机角色
Fsmo maintenance: transfer infrastructure master //转移基础结构主机角色

抢占
当 Primary DC 出现故障时，就不能进行转移操作了，只能占用操作主机，操作过程同上，只是把 transfer 改为 seize

>get-ADforest //查看域林信息
>netdom query fsmo //查看操作主机角色

修改域控 IP

1.直接在网卡配置里修改 IP
2.命令行里操作：
>net stop NETLOGON
>net start NETLOGON
>ipconfig /registerdns

3.打开 DNS 服务器管理控制台，删除所有和原 IP 相关的 A 记录

重命名域控制器

>netdom computername dc.cof.com /enumerate //查看 DC 的所有 FQDN 名称
>netdom computername dc.cof.com /add:newname.cof.com //添加新名称
>netdom computername dc.cof.com /makeprimary:newname.cof.com
重启域控制器
>netdom computername newname.cof.com /remove:dc.cof.com //删除原来名字

>netdom computername dc.cof.com /enumerate //查看
删除原来的 DNS 记录（正向查找区域）

允许域用户将计算机加入域的数量

*默认每个域用户可将 10 台计算机加入域，自定义设置：
Win+R 输入 adsiedit.msc //打开 ADSI 编辑器
右击“ADSI 编辑器”→连接到→默认命名上下文→右击 DC=cof,DC=com→属性→
ms-DS-MachineAccountQuota→值为 0~65535 表示用户可加入域的计算机数

*或者单独委派用户加域权限
打开 Active Directory 用户和计算机→右击域名→委派控制→下一步，添加用户→下一步，将计算机加域→完成

查看用户修改密码的时间

Active Directory 用户和计算机→选中用户→双击属性→属性编辑器下边底部→pwdLastSet 即为最近修改密码的时间
-LastLogon 最后一次登录时间

AD 域控相关端口号

端口号	tcp/udp	服务
53	t/u	DNS
88	t/u	Kerberos
123	u	NTP
135	t	Rpc Endpoint Master （msrpc）
137	u	NetBIOS Name Service
138	u	NetBIOS Datagram Service
139	t/u	NetBIOS session Service （netbios-ssn）
389	t/u	LDAP
445	t	SMB (CIFS) （microsoft-ds）
464		Kpasswd5
593		ncacn_http （msrpc over HTTP 1.0）
636	u/t	LDAPS （tcpwrapped Ldap over SSL）
2179		vmrdp
3268	t	LDAP GC （Global Catalog）
3269	t	LDAPS GC （Global Catalog over SSL）

域策略

1.允许指定用户远程登录到计算机

*计算机→策略→Windows 设置→安全设置→本地策略→用户权限分配
　　允许通过终端服务登录：添加远程用户组(Remote Desktop Users 和 Domain Admins）
*计算机→首选项→控制面板选项→本地用户和组
　　组名：Remote Desktop Users(内置) 添加远程用户进去

2.允许指定用户从本地登录到计算机

*计算机→策略→Windows 设置→安全设置→本地策略→用户权限分配
　　允许本地登录：添加指定用户或组

3.用户密码输错 3 次锁定 5 分钟

*计算机→策略→Windows 设置→安全设置→帐户策略→帐户锁定策略

在此后重置帐户锁定计数器	5 分钟
帐户锁定时间	5 分钟
帐户锁定阈值	3 次无效登录

4.十五分钟无操作自动锁屏

*用户→策略→管理模板→控制面板→个性化

带密码的屏幕保护程序	已启用
屏幕保护程序超时	已启用 900 秒
启用屏幕保护程序	已启用

5.将指定用户加入到计算机的某个组

*计算机→首选项→控制面板设置→本地用户和组
　　组名：xxxx(内置)→本地组→操作为更新→组名 xxxx，添加成员

6.将登录到计算机的用户添加到该计算机的某个组

*用户→首选项→控制面板设置→本地用户和组
　　组名：xxxx(内置)→本地组→操作为更新→组名 xxxx

7.设置计算机的组策略后台更新时间

*计算机→策略→管理模板→系统→组策略

设置计算机的组策略刷新间隔　　15 分钟　随机时间 5 分钟

设置域控制器的组策略刷新间隔　　15 分钟　随机时间 5 分钟

8.映射网络磁盘 S 盘给指定用户（用户登录后自动挂载共享磁盘）

*用户→首选项→Windows 设置→驱动器映射

S：属性信件 S，位置\\dc\sharepool

常用→项目级别目标：安全组

9.允许 ping 包入站（icmp echo request 入站）

*计算机→策略→管理模板→网络→网络连接→Windows 防火墙→域配置文件

Windows 防火墙→允许 icmp 例外：允许传入回显请求

10.禁止用户更改计算机系统时间

*计算机→策略→Windows 设置→安全设置→本地策略→用户权限分配

更改时区　　空（无用户）

更改系统时间　　空（无用户）

11.指定域用户的桌面（墙纸）

*用户→策略→管理模板→桌面→Active Desktop

启用 Active Desktop　　已启用

桌面墙纸　　\\dc\share\desktop.jpg　　平铺

12.用户登录时运行指定的程序

*用户→策略→管理模板→系统→登录

在用户登录时运行这些程序　　添加指定程序

13.用户登录时运行指定的脚本

*用户→策略→Windows 设置→脚本→登录

名称：脚本文件名　　脚本文件位于 DC 上的：

C:\Windows\SYSVOL\sysvol\域名\Policies\{组策略唯一 ID}\User\Scripts\Logon 里

14.受限制的组（只有指定的用户才在该组里）

*计算机→策略→Windows 设置→安全设置→受限制的组

组名 BULTIN\Administrators　　成员：指定的用户

15.用户文件夹重定向到 D 盘或服务器上

*用户→策略→Windows 设置→文件夹重定向→（选桌面和/或文档）

基本（重定向所有人的文件夹到相同位置）路径 D:\%username%\desktop

或 documents

16.漫游用户配置文件

*计算机→策略→管理模板→系统→用户配置文件

为正在登录此计算机的所有用户设置漫游配置文件路径：

已启用 \\dc\share\%username%

17.允许多个用户同时远程登录计算机（加授权）

*计算机→策略→管理模板→Windows 组件→远程桌面服务→远程桌面会话主机→连接

限制连接的数量　　允许的 RD 最大连接数　100

将远程桌面服务用户限制到单独的远程桌面服务会话　　已启用

为远程桌面服务用户会话远程控制设置规则　　已启用 不经用户授权完全控制

*计算机→策略→管理模板→Windows 组件→远程桌面服务→远程桌面会话主机→授权

设置远程桌面授权模式　　按用户

使用指定的远程桌面许可证服务器　　dc.cof.com

//加了域的主机，仅允许网络级别身份验证的远程桌面的计算机连接，所以 RDP 客户端计算机要求也要在域中，如果不在域中，那么服务端计算机要安装远程桌面服务的“远程桌面会话主机”角色，并指定授权服务器

18.无须按下 Ctrl+Alt+Del 登录

*计算机→策略→Windows 设置→安全设置→本地策略→安全选项→交互式登录

交互式登录　　已启用：无须按 Ctrl+Alt+Del

19.不显示最后登录的用户名

*计算机→策略→Windows 设置→安全设置→本地策略→安全选项→交互式登录

交互式登录　　已启用：不显示最后的用户名

20.域用户密码策略

*计算机→策略→Windows 设置→安全设置→帐户策略→密码策略

密码最长期限　　300 天
强制密码历史　　无
最短密码期限　　0 天
最短密码长度　　8 字符

*计算机→策略→Windows 设置→安全设置→本地策略→安全选项→交互式登录

交互式登录　　提示用户在密码过期之前更改密码　10 天

21.允许指定用户关闭计算机（含重启）

*计算机→策略→Windows 设置→安全设置→本地策略→用户权限分配

关闭系统　　添加指定的用户
从远程系统强制关机　　添加指定的用户

22.用户注销时清除最近打开过的文档记录

*用户→策略→管理模板→“开始”菜单和任务栏

退出系统时清除最近打开的文档的历史　　已启用

23.计算机启动时自动部署安装软件

*计算机→策略→软件设置→软件安装

新建数据包　使用网络路径　　//软件包必须为.msi 的安装包

24.配置防火墙规则

*计算机→策略→Windows 设置→安全设置→高级安全 Windows 防火墙

出入站规则　　新建 xxx

*计算机→策略→管理模板→网络→BranchCache

启用 BranchCache　　已启用

25.发布通告消息给用户（用户登录界面上显示）

*计算机→策略→Windows 设置→安全设置→本地策略→安全选项→交互式登录

试图登录的用户的消息标题　　标题内容
试图登录的用户的消息文本　　消息内容

26.禁止管理人员修改 IP（网络配置）

*计算机→策略→Windows 设置→安全设置→系统服务

选择 Network Connections，手动，删除指定用户 everyone 之类的完全控制权限

*用户→策略→管理模板→“开始”菜单和任务栏

删除网络图标　　已启用

*用户→策略→管理模板→网络→网络连接

禁止访问 LAN 连接的属性　　已启用

27.禁止用户使用外部存储设备（U 盘）

*用户→策略→管理模板→系统→可移动存储访问

可移动磁盘：拒绝读取权限　　已启用

可移动磁盘：拒绝访问权限　　已启用　　//重启生效

28.远程桌面会话时间限制

*计算机→策略→管理模板→Windows 组件→远程桌面服务→远程桌面会话主机→会话时间限制

设置活动但空闲的远程桌面服务会话时间限制　　已启用 30 分钟（到时断开）

设置活动的远程桌面服务会话的时间限制　　已启用 总时间 2 小时

设置已中断会话的时间限制　　已启用 10 分钟（到时结束会话

默认情况下远程桌面服务允许用户断开会话而不注销和结束会话，会话处于断开状态时，用户运行的程序仍保持活动。

29.远程连接时允许音频重定向至客户端

*计算机→策略→管理模板→Windows 组件→远程桌面服务→远程桌面会话主机→设备和资源重定向

允许音频和视频播放重定向　　已启用（serv→clnt）

允许音频录制重定向　　已启用（clnt→serv）

*计算机→策略→管理模板→Windows 组件→远程桌面服务→远程桌面会话主机→剪帖板重定向或 即插即用设备重定向

30.配置 Windows 自动更新

*计算机→策略→管理模板→Windows 组件→Windows 更新

配置自动更新　　4-自动下载并计划安装计划安装日期，时间，默认会重启

始终在计划的时间重新启用　　为用户预留 15 分钟

自动更新检测频率　　24 小时
允许非管理员接收更新通知　　已启用

31.启动远程桌面服务

*计算机→策略→Windows 设置→安全设置→系统服务
Remote Desktop Services　　自动
*计算机→管理模板→Windows 组件→远程桌面服务→远程会话主机→连接
允许用户通过使用远程桌面服务进行远程连接
*计算机→策略→Windows 设置→安全设置→高级安全 Windows 防火墙
入站规则：　　允许远程桌面服务入站

32.关闭本地组策略对象处理

*计算机→策略→管理模板→系统→组策略
关闭本地组策略对象处理：　　已启用
//表示不使用计算机本地的组策略，只应用域控下发的策略