# Dcpromo

用于将windows 2000和windows server 2003独立服务器和成员服务器转为AD服务器的可执行文件。

安装过程中将会发生以下更改：

* 服务器从基于注册表的账户数据库（SAM）转换为基于可扩展存储引擎（ESE）的目录。而从NT4.0 DC升级，SAM中的账户将迁移到AD服务器中。
* 对于新安装，AD数据库从\SYSTEM32中NTDS.DIT模板文件创建。  
  成立新管理员账号，新密码，新SID。旧管理账号停用。
* 在NTFS格式驱动器指定位置创建新的层级文件夹，称为System Volume。  
  SYSVOL目录树创建，托管策略及登陆脚本。  
  NETLOGON与SYSVOL创建共享。  
  从NT4.0升级，原NETLOGON共享文件移至SYSVOL树中。
* Win32时间服务进行同步。  
  FRS（File Replication Service)服务改为自动，KDC（Key Distributing Center)服务设置为自动启动。
* 可以降级。

# 检查System Volume

Sysvol的创建及其结构，AD活动目录。

## AD数据库文件

### Sysvol（Shared System Volume)

* SYSVOL Share  
  托管策略，脚本文件夹。由Netlogon服务自动共享。
* NETLOGON Share  
  托管Window2000网络客户端的登录、注销、启动和关闭脚本。
* File System Junctions  
  将目标文件系统位置的名称空间移植到NTFS卷
* Windows 2000 Default Group Policies  
  默认域策略和默认DC是唯一的默认策略。管理员稍后可以创建其他策略并复制到其他DC。
* FRS Staging Directories

SYSVOL文件夹默认位置为systemroot/sysvol，不过管理员可以指定位置，因此解决问题时注意文件位置。

### NTDS.DIT 和Log Files

安装AD服务会创建一个数据库及数据库日志文件

Ntds.dit是一个Jet Database。包含了AD的所有信息，包含所有objects，schema，global catalog。

该文件位置在安装时可选，默认为%SYSTEMROOT%/Ntds。

将数据库与日志文件放在不同的物理硬盘上将提供更好的性能。

## 从Windows NT 4.0升级到Windows 2000的Netlogon问题

PDC会是第一台升级的电脑，通常运行WINNT32.EXE来启动，完成升级后Dcpromo会启动并提示操作者创建DC。

在Dcpromo期间，Netlogon文件夹从REPL\EXPORT\SCRIPTS移动到\SYSVOL\SYSVOL\%FQDM%\SCRIPTS文件夹。

FRS不会复制留在域中由NT 4.0使用的旧LMREPL服务。

## 验证是否安装成功

1. 在Event Viewer中查看安装启动过程  
   查看与安装启动有关的error和warning消息。  
   确认Sysvol和Netlogon文件夹是否被创建并共享。  
   运行**net view \\<domain controller name> 或 net share**查看是否在列表中
2. 运行 Dcdiag /v  
   查看日志文件是否通过所有检查。  
   \*客户端无法正确解析域的DNS记录。  
   客户端必须指向该域的DNS服务器。  
   \*提供的凭据与正在使用的冲突。  
   客户端已打开与域中服务器连接，比如mapped drivers。
3. 查看Fully Qualified Computer Name  
   在Command prompt输入net config rdr
4. 查看Service Startup  
   Computer Management-->Services
5. 禁用不必要的服务  
   设置为Manual或Disabled，包括：  
   The Print Spooler service  
   Messenger and alerter services在所有服务器上
6. Run Netdiag  
   Command prompt中输入**netdiag /v >c:\netdiag.<mmddyy>.txt**查看文件中网络连接，DNS、WINS注册  
   将此文件保存并更新到所有服务器的本地文件夹，以便后续查看。
7. 使用windows 2000备份DS及Key Services；开发维护DS及其他关键服务备份。
8. 规划EFS Recovery Policy  
   A plan for storage and recovery of EFS certificates and private keys.
9. 验证Group Policy是否应用  
   在Application event log搜索1704，确认成功应用。

# 检查Dcpromo中使用的日志文件

默认位置：%SYSTEMROOT%\Debug，记录了安装删除的实际过程。

安装或删除AD出现问题的两个主要原因：

1. Lack of good DNS name resolution
2. Lack of necessary network connectivity(Firewalls, ports being shutdown, etc)

\* 221254: Registry Settings for Event Detail in the Dcpromoui.log File.

## DcpromoUI.log

从开始到结束，用户选择和操作的详细进度。错误消息，成功确认消息。

还包含：

* 用于复制的源DC名称
* 复制到目标服务器的Directory partitions
* 每个Directory partitions复制的项目数
* 目标DC上配置的服务
* 注册表和文件设置的ACEs
* SYSVOL目录
* Applicable error messages
* 安装期间管理员输入的applicable selections

## Dcpromo.log

关键操作摘要。

记录设置：

* Site name
* Path for AD database and log files
* Time synchronization
* 账户信息

记录以下创建：

* AD database
* SYSVOL trees
* 安装，修改服务

## Netsetup.log

尝试加入域的消息以及任何可能导致加入失败的错误消息。

\*Domain join problem

客户端无法正确解析域的DNS记录，客户端必须指向a DNS server hosting the zone for that domain.

## Dcpromos.log

用户在GUI模式下设置时进行记录。

# 检查DNS与AD集成

DNS域与AD域对不同的命名空间使用相同的域名。

## DNS与AD域的集成

客户端计算机必须能够定位DC，来获取AD服务。

使用A resource record and SRV records。

A Resource record: FQDN, IP address

SRV: FQDN, Service

## 什么是Active Directory Integrated Zones

将DNS zone集成入AD数据库中。该区域是资源记录的逻辑分组，允许这些记录以一个unit进行zone transfers。

AD Integrated Zones作为对象存储与AD数据库中，若存储于domain partition则将复制到该域的所有DC中

## Active Directory Integrated Zones的优势

* Multi-master Replication