

第9章 AD DS 数据库的复制

对拥有多台域控制器的AD DS域来说，如何有效率的复制AD DS数据库、如何提高AD DS的可用性与如何让用户能够快速登录，是系统管理员必须要了解的重要课题。

- ▼ 站点与AD DS数据库的复制
- ▼ 默认站点的管理
- ▼ 利用站点来管理AD DS复制
- ▼ 管理全局编录服务器
- ▼ 解决AD DS复制冲突的问题

9.1 站点与AD DS数据库的复制

站点 (site) 是由一或多个IP子网 (subnet) 所组成, 这些子网之间通过**高速且可靠的连接**互连起来, 也就是这些子网之间的连接速度要够快且稳定、符合你的需要, 否则就应该将它们分别规划为不同的站点。

一般来说, 一个LAN (局域网) 之内各个子网之间的连接都符合速度且高可靠的要求, 因此可以将一个LAN规划为一个站点; 而WAN (广域网) 内各个LAN之间的连接速度一般都不快, 因此WAN之中的各个LAN应分别规划为不同的站点, 参见图9-1-1。

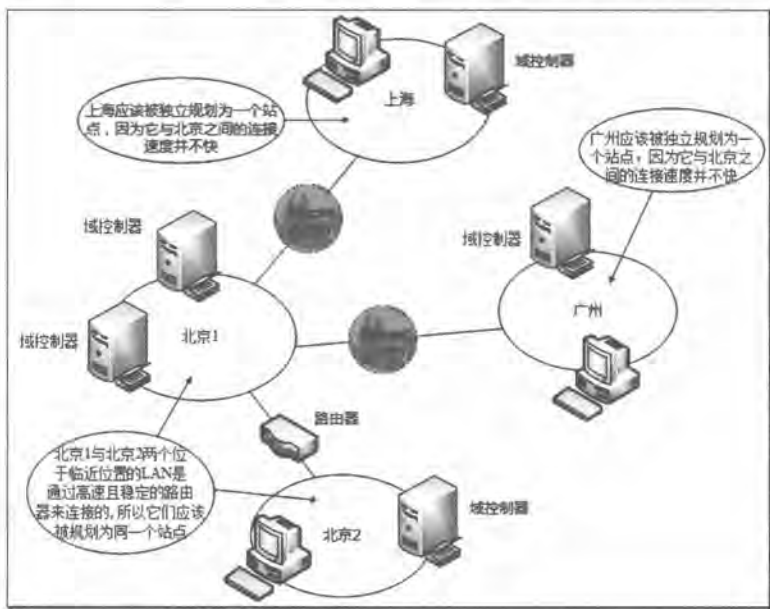


图 9-1-1

AD DS内大部分数据是利用**多主机复制模式** (multi-master replication model) 来复制。在这种模式之中, 可以直接更新任何一台域控制器内的AD DS对象, 之后这个更新对象会被自动复制到其他域控制器, 例如当在任何一台域控制器的AD DS数据库内新建一个用户账户后, 这个账户会自动被复制到域内的其他域控制器。

站点与AD DS数据库的复制之间有着重要的关系, 因为这些域控制器是否在同一个站点, 会影响到域控制器之间AD DS数据库的复制行为。

9.1.1 同一个站点之间的复制

同一个站点内的域控制器之间是通过快速的连接互连在一起的, 因此在复制AD DS数据



库时，可以有效、快速地复制，而且不会压缩所传送的数据。

同一个站点内的域控制器之间的AD DS复制采用**更改通知**（change notification）的方式，也就是当某台域控制器（以下将其称为**源域控制器**）的AD DS数据库内有一笔数据更改时，默认它会等15秒后，就通知位于同一个站点内的其他域控制器。收到通知的域控制器如果需要这笔数据的话，就会给**源域控制器**发出**更新信息**的请求，这台**源域控制器**收到请求后，便会开始复制的过程。

1. 复制伙伴

源域控制器并不是直接将改动数据复制给同一个站点内的所有域控制器，而是只复制给它的**直接复制伙伴**（direct replication partner），然而哪些域控制器是其**直接复制伙伴**呢？每一台域控制器内都有一个被称为Knowledge Consistency Checker（KCC）的程序，它会自动建立最有效率的**复制拓扑**（replication topology），也就是决定哪些域控制器是它的**直接复制伙伴**、而哪些域控制器是它的**转移复制伙伴**（transitive replication partner），换句话说，**复制拓扑**是复制AD DS数据库的逻辑连接路径，如图9-1-2所示。

以图中域控制器DC1来说，域控制器DC2是它的**直接复制伙伴**，因此DC1会将变动数据直接复制给DC2，而DC2收到数据后，会再将它复制给DC2的**直接复制伙伴**DC3，依此类推。

对域控制器DC1来说，除了DC2与DC7是它的**直接复制伙伴**外，其他的域控制器（DC3、DC4、DC5、DC6）都是**转移复制伙伴**，它们是间接获得由DC1复制来的数据。

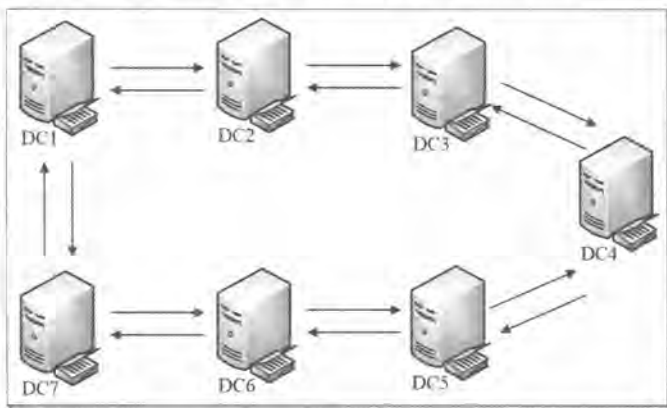


图 9-1-2

2. 如何减少复制延迟时间

为了减少复制延迟的时间（replication latency），也就是从**源域控制器**内的AD DS数据有变动开始，到这些数据被复制到所有其他域控制器之间的间隔时间要尽量缩短，因此KCC在

建立复制拓扑时，会让数据从源域控制器传送到目的域控制器时，其所跳跃的域控制器数量（hop count）不超过3台，以图9-1-2来说明，从DC1到DC4跳跃了3台域控制器（DC2、DC3、DC4），而从DC1到DC5也只跳跃了3台域控制器（DC7、DC6、DC5）。换句话说，KCC会让源域控制器与目的域控制器之间的域控制器数量不超过两台。

附注

为了避免源域控制器负担过重，因此源域控制器并不是同时通知其所有的直接复制伙伴，而是会间隔3秒，也就是先通知第1台直接复制伙伴，间隔3秒后再通知第2台，依此类推。

当有新域控制器加入时，KCC会重新建立复制拓扑，而且仍然会遵照跨越的域控制器数量不超过3台的原则，例如当图9-1-2中新建了一台域控制器DC8后，其复制拓扑就会有变化，图9-1-3为可能的复制拓扑之一，图中KCC将域控制器DC8与DC4设置为直接复制伙伴，否则DC8与DC4之间，无论是通过【DC8→DC1→DC2→DC3→DC4】或【DC8→DC7→DC6→DC5→DC4】的途径，都会违反跨越的域控制器数量不超过3台的原则。

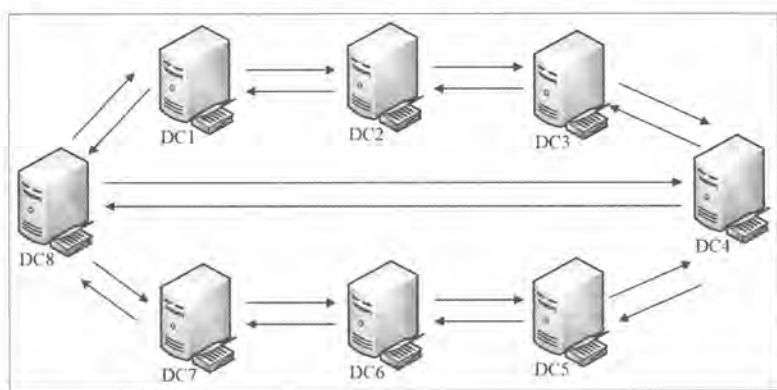


图 9-1-3

3. 紧急复制

对某些重要的更新数据来说，系统并不会等15秒钟才通知其直接复制伙伴，而是立刻通知，这个操作被称为紧急复制。这些重要的更新数据包含用户账户被锁定、账户锁定策略更改、域的密码策略更改等。

9.1.2 不同站点之间的复制

由于不同站点之间的连接速度不够快，因此为了降低对连接带宽的影响，故站点之间的 AD DS 数据在复制时会被压缩，而且数据的复制是采用计划任务（schedule）的方式，也就是



在定义好的任务时间内才会进行复制工作。原则上应该尽量避开站点链接的网络负载高峰阶段，安排在离峰时期执行复制工作，同时复制频率也不要太高，以避免复制时占用两个站点之间的连接带宽，影响两个站点之间其他数据的传输效率。

不同站点的域控制器之间的**复制拓扑**，与同一个站点的域控制器之间的**复制拓扑**是不相同的。每一个站点内都各有一台被称为**站点间拓扑生成器**的域控制器，它负责建立**站点之间的复制拓扑**，并从其站点内挑选一台域控制器来扮演**bridgehead服务器**（桥头服务器）的角色，例如图9-1-4中SiteA的DC1与SiteB的DC4，两个站点之间在复制AD DS数据时，是由这两台**bridgehead服务器**负责将该站点内的AD DS变动数据复制给对方，这两台**bridgehead服务器**得到对方的数据后，会再将它们复制给同一个站点内的其他域控制器。

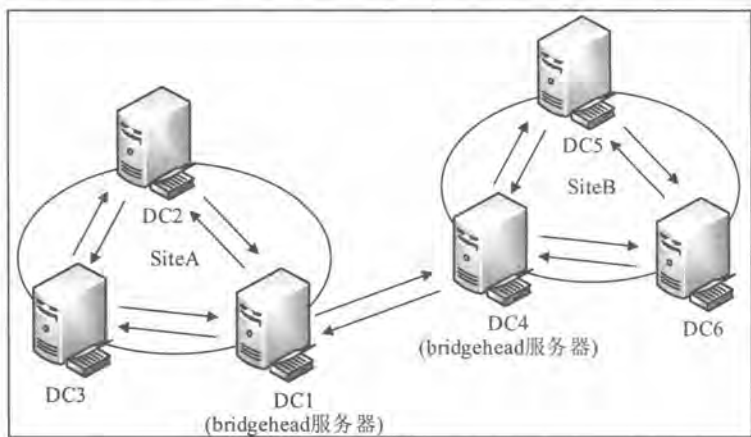


图 9-1-4

两个站点之间AD DS复制的其他细节，包含**站点链接**（site link）、开销、复制任务、复制频率等都会在后面章节另外说明。

9.1.3 目录分区与复制拓扑

AD DS数据库被逻辑的分为以下多个目录分区（详见第1章）：**架构目录分区**、**配置目录分区**、**域目录分区**与**应用程序目录分区**。

KCC在建立**复制拓扑**时，并不是整个AD DS数据库只采用单一**复制拓扑**，而是不同的目录分区各有其不同的**复制拓扑**，例如DC1在复制**域目录分区**时，可能DC2是它的直接复制伙伴，但是在复制**配置目录分区**时，DC3才是它的直接复制伙伴。

9.1.4 复制通信协议

域控制器之间在复制AD DS数据时，其所使用的复制通信协议分为以下两种。



➤ **RPC over IP (Remote Procedure Call over Internet Protocol)**

无论是同一个站点内或不同站点之间，都可以利用RPC over IP来执行AD DS数据库的复制操作。为了确保数据在传送时的安全性，RPC over IP会执行验证身份与数据加密的工作。

附注

在**Active Directory**站点和服务控制台中，同一个站点之间的复制通信协议RPC over IP字样会被改用IP字样来代表。

➤ **SMTP (Simple Mail Transfer Protocol)**


SMTP只能够用来执行不同站点之间的复制。如果不同站点的域控制器之间无法直接通信，或之间的连接质量不稳定时，就可以通过SMTP来传输。不过这种方式有些限制，例如：

- 只能够复制架构目录分区、配置目录分区与应用程序目录分区，不能复制域目录分区。
- 需向企业CA (Enterprise CA) 申请证书，因为在复制过程中，需要利用证书来进行身份验证。

9.2 默认站点的管理

在建立第一个域（林）时，系统就会自动建立一个默认站点，以下介绍如何来管理这个默认的站点。

9.2.1 默认的站点

可以利用【单击左下角开始图标→**Windows 管理工具**→**Active Directory站点和服务**】的方法来管理站点，如图9-2-1所示。

- **Default-First-Site-Name:** 这是默认的的第一个站点，它是在建立AD DS林时由系统自动建立的站点，可以更改这个站点的名称。
- **Servers:** 其中记录着位于此Default-First-Site-Name站点内的域控制器与这些域控制器的设置值。
- **Inter-Site Transports:** 记录着站点之间的IP与SMTP这两个复制通信协议的设置值。
- **Subnets:** 可以通过此处在AD DS内建立多个IP子网，并将子网划入到所属的站点内。



图 9-2-1

假设在AD DS内已经建立了多个IP子网，此时在安装域控制器时，如果此域控制器是位于其中某个子网内（从IP地址的网络ID来判断），则此域控制器的计算机账户就会自动被放到此子网所隶属的站点内。

然而在建立AD DS林时，系统默认并没有在AD DS内建立任何的子网，因此所建立的域控制器就不属于任何一个子网，此时这台域控制器的计算机账户会被放到Default-First-Site-Name站点内，例如图9-2-1中的DC1、DC2、……、DC6等域控制器都是在此站点内。

9.2.2 Servers文件夹与复制设置

图9-2-1中的Servers文件夹内记录着位于Default-First-Site-Name站点内的域控制器，而在选择图中的任何一台域控制器后（例如DC2），将出现如图9-2-2所示的界面。

图中的NTDS Settings内包含选择两个由KCC所自动建立的**连接对象**（connection object），其名称都是**自动产生**，这两个**连接对象**分别来自DC1与DC3，表示DC2会直接接收由这两台域控制器所复制过来的AD DS数据，也就是说这两台域控制器都是DC2的**直接复制伙伴**。同理在点取其他任何一台域控制器时，也可以看到它们与**直接复制伙伴**之间的**连接对象**。

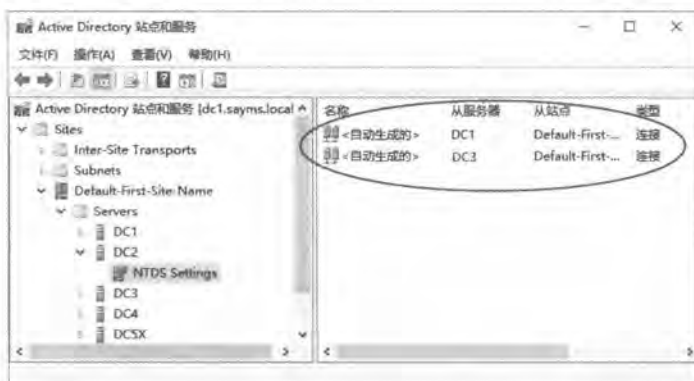


图 9-2-2



这些在同一个站点内的域控制器相互之间的**连接对象**，都会由KCC负责自动建立与维护，而且是双向的。也可以根据需求来手动建立**连接对象**，例如假设图9-2-3中DC3与DC6之间原本并没有**连接对象**存在，也就是它们并不是**直接复制伙伴**，但是可以手动在它们之间建立单向或双向的**连接对象**，以便让它们之间可以直接复制AD DS数据库，例如图中手动建立的**连接对象**是单向的，也就是DC6单向直接从DC3来复制AD DS数据库。

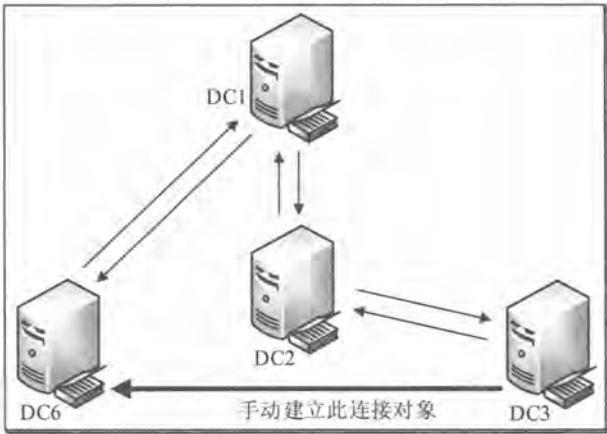


图 9-2-3

建立此单向连接对象的方法为【如图9-2-4所示选中DC6之下的NTDS Settings并右击**新建Active Directory域服务连接**选择DC3……】。



图 9-2-4

在双击图9-2-2右侧的任何一个**连接对象**后（例如源服务器为DC1的那一个），将出现如图9-2-5所示的界面。可以单击图中**服务器**右侧的**更改**按钮，来改变复制的源服务器。



图 9-2-5

如果域控制器的AD DS数据有变动时（例如新建用户账户），则其默认是15 秒钟后会通知同一个站内的**直接复制伙伴**，以便将数据复制给它们。即使没有数据变动，默认也会每隔一小时执行一次复制工作，以确保没有遗失任何应该复制的数据，可以通过如图9-2-5所示中的**更改计划**按钮来查看与更改此间隔时间，如图9-2-6所示。

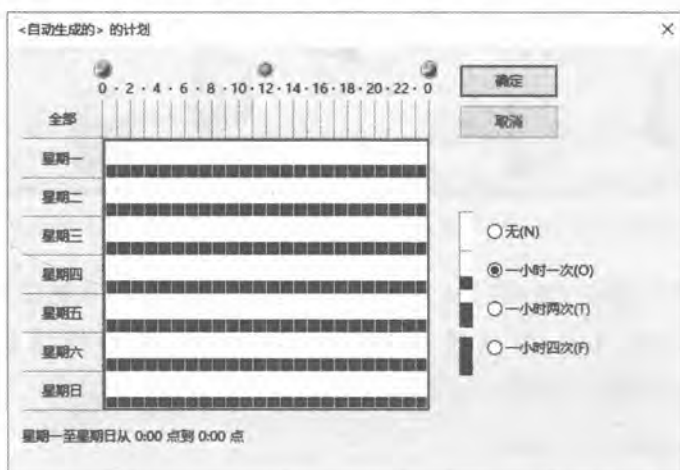


图 9-2-6

如果想要立刻复制的话，请自行以手动的方式来完成：**【先选择图9-2-7左侧的目的服务器（例如DC2）➡单击NTDS Settings➡选中右侧的复制来源服务器并右击➡立即复制】**，图中表示立刻从DC1复制到DC2。



图 9-2-7

9.3 利用站点来管理AD DS复制

以下将先利用图9-3-1来说明如何建立多个站点与IP子网，然后再说明站点之间的AD DS复制设置。

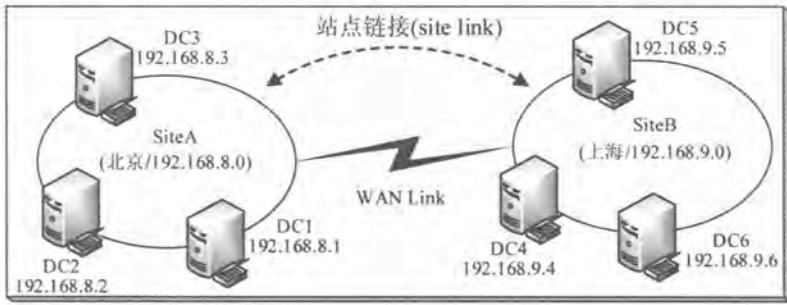


图 9-3-1

站点之间除了物理链接（WAN link）外，还必须建立逻辑的**站点链接**（site link）才能进行AD DS数据库的复制，而系统默认已经为IP复制通信协议建立一个名称为DEFAULTIPSITELINK的站点链接，如图9-3-2所示。



图 9-3-2



我们在建立图9-3-1中的SiteA与SiteB时，必须通过**站点链接**将这两个站点逻辑的连接在一起，它们之间才能进行AD DS数据库的复制。

9.3.1 建立站点与子网

以下将先建立新站点，然后建立隶属于此站点的IP子网。

1. 建立新站点

我们将说明如何建立图9-3-1中的SiteA与SiteB。

STEP 1 单击左下角开始图标 Windows 管理工具 Active Directory 站点和服务 如图9-3-3所示选中Sites并右击 新站点。



图 9-3-3

STEP 2 在图9-3-4中设置站点名称（例如SiteA），并将此站点归纳到适当的**站点链接**后单击**确定**按钮。图中因为目前只有一个默认的**站点链接**DEFAULTIPSITELINK，故只能暂时将其归纳到此默认的**站点链接**。只有隶属于同一个**站点链接**的站点之间才能进行AD DS数据库的复制。



图 9-3-4

STEP 3 在图9-3-5中直接单击**确定**按钮。



图 9-3-5

STEP 4 请重复STEP 1到STEP 3来建立SiteB，图 9-3-6为完成后的界面。



图 9-3-6

2. 建立 IP 子网

以下将说明如何建立图9-3-1中的IP子网192.168.8.0与192.168.9.0，并将它们分别划入到SiteA与SiteB内。

STEP 1 如图9-3-7所示【选中Subnets并右击新建子网】。



图 9-3-7

STEP 2 在图9-3-8中的前缀处输入192.168.8.0/24，其中的192.168.8.0为网络ID，而24表示子网掩码为255.255.255.0（二进制中1的位数共有24个），并将此子网划入站点SiteA内。



图 9-3-8

STEP 3 重复前两个步骤来建立IP子网192.168.9.0，并将其划入站点SiteB。图9-3-9为完成后的界面。



图 9-3-9

9.3.2 建立站点链接

以下将说明如何建立图9-3-1中的站点链接，并将此站点链接命名为SiteLinkAB。我们利用IP复制通信协议来说明。

注意



由于我们在前面建立 SiteA 与 SiteB 时，都已经将 SiteA 与 SiteB 归纳到 DEFAULTIPSITELINK 这个站点链接，也就是说这两个站点已经通过 DEFAULTIPSITELINK 逻辑的连接在一起了。我们通过以下练习来将其改为通过 SiteLinkAB 来连接。

STEP 1 请如图9-3-10所示【选中IP并右击➡新站点链接】。



图 9-3-10

STEP 2 在图9-3-11中【设置站点链接名称（例如SiteLinkAB）➡选择SiteA与SiteB后单击添加按钮➡单击确定按钮】。之后SiteA与SiteB便可根据站点链接SiteLinkAB内的设置来复制AD DS数据库。



图 9-3-11

STEP 3 图9-3-12为完成后的界面。



图 9-3-12



9.3.3 将域控制器移动到所属的站点

目前所有的域控制器都被放置到Default-First-Site-Name站点内，而在完成新站点的建立后，我们应将域控制器移动到正确的站点内。以下假设域控制器DC1、DC2与DC3的IP地址的网络标识符都是192.168.8.0（如图9-3-13所示），故需将DC1、DC2与DC3移动到站点SiteA；同时假设DC4、DC5与DC6的IP地址的网络标识符都是192.168.9.0，故需将DC4、DC5与DC6移动到站点SiteB。

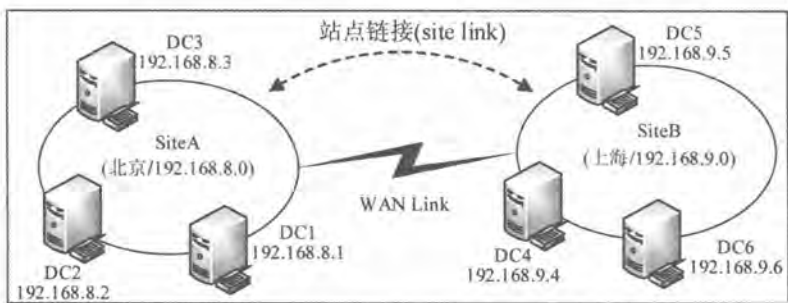


图 9-3-13

注意

以后如果在图9-3-13中的北京网络内安装新域控制器的话，则该域控制器的计算机账户会自动被放置到SiteA内，同理在上海网络内所安装的新域控制器，其计算机账户会自动被放到SiteB内。

STEP 1 如图9-3-14所示【展开Default-First-Site-Name站点➤单击Servers➤选中要被移动的服务器（例如DC1）并右击➤移动】。



图 9-3-14

STEP 2 在图9-3-15选择目标站点SiteA后单击确定按钮。



图 9-3-15

STEP 3 重复以上步骤将DC2、DC3移动到SiteA、将DC4、DC5与DC6移动到SiteB。图9-3-16为完成后的界面。



图 9-3-16

附注

可以在SiteA与SiteB之间搭建一台由Windows Server所扮演的路由器，来模拟演练SiteA与SiteB是位于两个不同网络的环境。

9.3.4 指定首选的bridgehead服务器

前面说过每一个站点内都各有一台被称为**站点之间拓扑生成器**的域控制器，它负责建立**站点之间的复制拓扑**，并从其站点内挑选一台域控制器来扮演**bridgehead服务器**的角色，例如图9-3-17中SiteA的DC1与SiteB的DC4，两个站点之间在复制AD DS数据时，是由这两台**bridgehead服务器**负责将该站点内的AD DS变动数据复制给对方，这两台**bridgehead服务器**得到对方的数据后，会再将它们复制给同一个站点的其他域控制器。

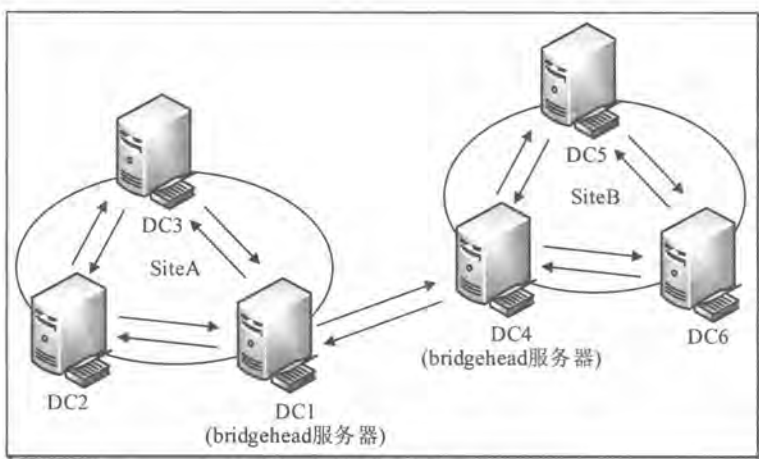


图 9-3-17

也可以自行选择扮演**bridgehead服务器**的域控制器，它们被称为**首选的bridgehead服务器**（preferred bridgehead server）。例如要将SiteA内的域控制器DC1指定为**首选的bridgehead服务器**的话：【请如图9-3-18所示展开站点SiteA⇨单击**Servers**⇨点选域控制器DC1⇨单击上方**属性**图标⇨选择要复制的通信协议（例如IP）⇨单击**添加**按钮】。



图 9-3-18

可以重复以上的步骤，来将多台域控制器设为**首选的bridgehead服务器**，但是AD DS一次只会从其中挑选一台来复制数据，若这一台出现故障了，它会再挑选其他的**首选的bridgehead服务器**。

若要查看**首选的bridgehead服务器**列表的话，也可以【展开**Inter-Site Transports**⇨对着IP右击⇨**属性**⇨选择**属性编辑器**选项卡⇨单击**筛选**按钮⇨选择**显示只读属性处的反向链接**⇨双击属性列表中的**bridgeheadServerListBL**】。

注意

非必要请不要自行指定首选的bridgehead服务器，因它会让KCC停止自动挑选bridgehead服务器，此时若所选择的首选的bridgehead服务器都出现故障时，KCC不会再自动挑选bridgehead服务器，如此将没有bridgehead服务器可供使用。

若要将扮演**首选的bridgehead服务器**的域控制器移动到其他站点的话，请先取消其**首选的bridgehead服务器**的角色后再移动。

9.3.5 站点链接与AD DS数据库的复制设置

两个站点之间是通过**站点链接**的设置，来决定如何复制AD DS数据库：如图9-3-19所示【选中站点链接（例如SiteLinkAB）并右击**属性**通过图9-3-20的界面来设置】。



图 9-3-19



图 9-3-20

- ✎ **更改站点链接中的站点成员：**可以在界面中将其他的站点加入到此站点链接 SiteLinkAB 内，也可以将站点从这个站点链接中删除。



➤ **开销 (cost)：**如果两个站点之间有多个物理的 WAN link，则它们之间就可以有多个逻辑的站点链接，而每一个站点链接可以有着不同的开销（默认值为100）。这里的开销是用来与其他站点链接相比较的相对值。每一个站点链接的开销计算，需要考虑到物理 WAN link 的连接带宽、稳定性、延迟时间与费用，例如若开销考虑是以 WAN link 的连接带宽为依据的话，则应该将带宽较大的站点链接的开销值设置得较低，假设将带宽较低的站点链接的开销设置为默认的100，则带宽较大的站点链接的开销值应该要比100小。KCC在建立复制拓扑，会选择站点链接开销较低的域控制器来当作直接复制伙伴。

另外，用户在登录时，如果其计算机所在的站点内没有域控制器可以提供服务的话（例如域控制器因故脱机），则用户的计算机会到其他站点去寻找域控制器，此时会通过站点链接开销最低的连接去查找域控制器，以便让用户能够快速登录。

➤ **复制频率为每...分钟、更改计划：**复制频率为每...分钟用来设置隶属于此站点链接的站点之间，每隔多长时间复制一次 AD DS 数据库，默认是180分钟。

但并不是时间到了就一定会执行复制工作，因还需看是否允许在此时间复制，此设置是通过前面图9-3-20的更改计划按钮，然后利用图9-3-21来更改计划。默认是一个星期7天、1天24小时的任何时段都允许进行复制，可以更改此计划，例如改为高峰时期不允许复制，不过它会增加复制的延迟时间。

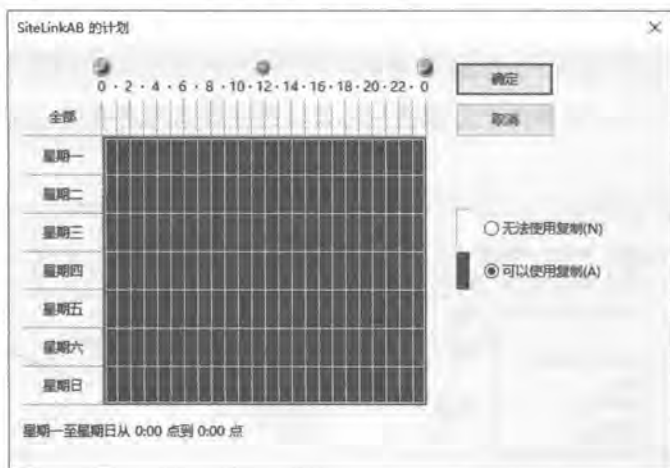


图 9-3-21

9.3.6 站点链接桥

站点链接桥 (site link bridge) 是由两个或多个站点链接所组成，它让这些站点链接具备转移性 (transitive)，例如图9-3-22中SiteA与SiteB之间已经建立了站点链接SiteLinkAB，而SiteB与SiteC之间也建立了站点链接SiteLinkBC，则站点链接桥SiteLinkBridgeABC让SiteA与SiteC之间具备着隐性的站点链接，也就是说KCC在建立复制拓扑时，可以将SiteA的域控制器DC1与SiteC的域控制器DC3设置为直接复制伙伴，让DC1与DC3之间可以通过两个WAN



link的物理链路，来直接复制AD DS数据，不需要由SiteB的域控制器DC2来转送。

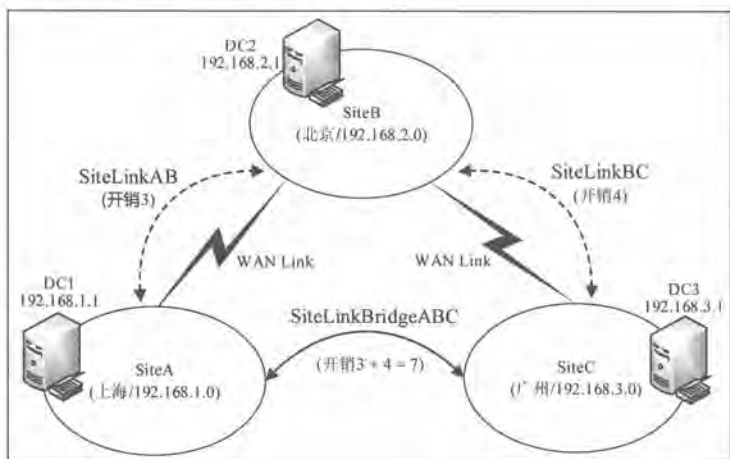


图 9-3-22

图中SiteLinkAB的开销为3、SiteLinkBC的开销为4，则SiteLinkBridgeABC的开销是 $3 + 4 = 7$ ，由于此开销高于SiteLinkAB的开销3与SiteLinkBC的开销4，因此KCC在建立复制拓扑，默认不会在DC1与DC3之间建立连接对象，也就是不会将DC1与DC3设置为直接复制伙伴，除非DC2无法使用（例如计算机故障、脱机）。

系统默认会自动桥接所有的站点链接，可以通过如图9-3-23所示【展开Inter-Site Transports 单击IP文件夹 单击上方属性图标 勾选或取消为所有站点链接搭桥】的方法来更改其设置值。



图 9-3-23

由于系统默认已经自动桥接所有的站点链接，因此不需要另外手动建立站点链接桥，除非想要控制AD DS数据复制的方向或两个站点之间受到限制无法直接通信，例如在图9-3-22的SiteB内搭建了防火墙，并通过防火墙限制SiteA的计算机不能与SiteC的计算机通信，则图中的SiteLinkBridgeABC就没有意义了，因为SiteA将无法直接与SiteC进行AD DS数据库复



制, 此时如果SiteA还可以通过另外一个站点SiteD来与SiteC通信的话, 我们就没有必要让KCC浪费时间建立SiteLinkBridgeABC, 或浪费时间尝试通过SiteLinkBridgeABC来复制AD DS数据库, 也就是说可以先取消勾选图9-3-23中的**为所有站点链接搭桥**, 然后如图9-3-24所示自行建立SiteLinkBridgeADC, 以便让SiteA的计算机与SiteC的计算机直接选择通过SiteLinkBridgeADC进行通信。



图 9-3-24

9.3.7 站点链接桥的两个范例讨论

1. 站点链接桥范例一

图9-3-25中SiteA与SiteB之间、SiteB与SiteC之间分别建立了**站点链接**, 并且分别有着不同的复制计划与复制频率, 请问DC1与DC3之间何时可以复制AD DS数据库(以下针对**域目录分区**来说明)?

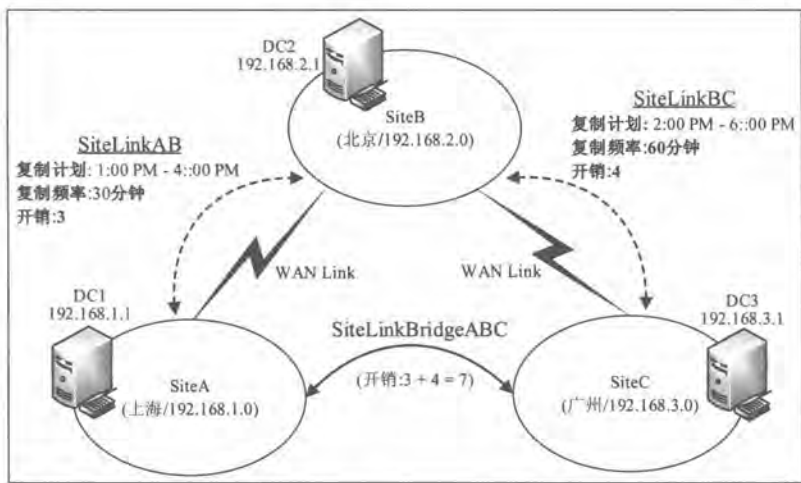


图 9-3-25



- ✎ 如果DC2正常工作，并且DC1、DC2与DC3隶属于同一个域

图中SiteLinkAB开销为3、SiteLinkBC开销为4，因此SiteLinkBridgeABC开销是 $3 + 4 = 7$ ，由于此开销高于SiteLinkAB的开销3与SiteLinkBC的开销4，因此KCC在建立复制拓扑时，并不会在DC1与DC3之间建立连接对象，也就是不会将DC1与DC3设为直接复制伙伴，所以DC1与DC3在复制AD DS数据库时必须通过DC2来传送。

当DC1的AD DS数据有变动时，它可以在1:00 PM ~ 4:00 PM之间将数据复制给DC2，而DC2在收到数据并存储到其AD DS数据库后，会在2:00 PM ~ 6:00 PM之间将数据复制给DC3。

- ✎ 如果DC2脱机，或DC2与DC1/DC3不是隶属于同一个域

此时因为DC2无法提供服务或不会存储不同域的AD DS数据，因此DC1与DC3之间必须直接复制AD DS数据库，此时KCC在建立复制拓扑时，因为SiteA与SiteC之间有站点桥接连接器，所以会在DC1与DC3之间建立连接对象，也就是将DC1与DC3设置为直接复制伙伴，让DC1与DC3之间可以直接复制。

但是何时DC1与DC3之间才会直接复制AD DS数据库呢？它们只有在两个站点链接的复制计划中有重叠的时段才会进行复制工作，例如SiteLinkAB复制计划是1:00 PM ~ 4:00 PM，而SiteLinkBC是2:00 PM ~ 6:00 PM，因此DC1与DC3之间会复制的时间为2:00 PM ~ 4:00 PM。

另外，DC1与DC3之间的复制间隔时间为两个站点链接的最大值，例如SiteLinkAB为30分钟，SiteLinkBC为60分钟，则DC1与DC3为两个站点链接的复制间隔时间为60分钟。

注意

在DC2故障或脱机（或DC2不是与DC1/DC3同一个域）的情况下，虽然可以通过站点桥接连接器让DC1与DC3直接复制AD DS数据库，但是如果两个站点链接的复制计划中没有重叠时段的话，则DC1与DC3之间还是无法复制AD DS数据库。

2. 站点链接桥范例二

如果图9-3-26中SiteA与SiteB之间、SiteB与SiteC之间分别建立了站点链接，但是却取消勾选前面图9-3-23中的桥接所有站点链接，且并没有自行建立站点桥接连接器，则DC1与DC3之间是否可以AD DS复制呢（以下针对域目录分区来说明）？

- ✎ 如果DC2正常工作，并且DC1、DC2与DC3隶属于同一个域

此时由于SiteA与SiteC之间没有站点桥接连接器，因此KCC在建立复制拓扑时，不会在DC1与DC3之间建立连接对象，也就是不会将DC1与DC3设为直接复制伙伴，因此DC1与DC3之间只能通过DC2来转发AD DS数据。

- ✎ 如果DC2脱机，或DC2与DC1/DC3不是隶属于同一个域

此时DC2无法接收与存储DC1与DC3的AD DS数据，因此DC1与DC3必须直接复制



AD DS数据，但是因为SiteA与SiteC之间并没有站点桥接连接器，因此KCC无法在DC1与DC3之间建立连接对象，也就是无法将DC1与DC3设为直接复制伙伴，所以DC1与DC3之间将无法复制AD DS数据。

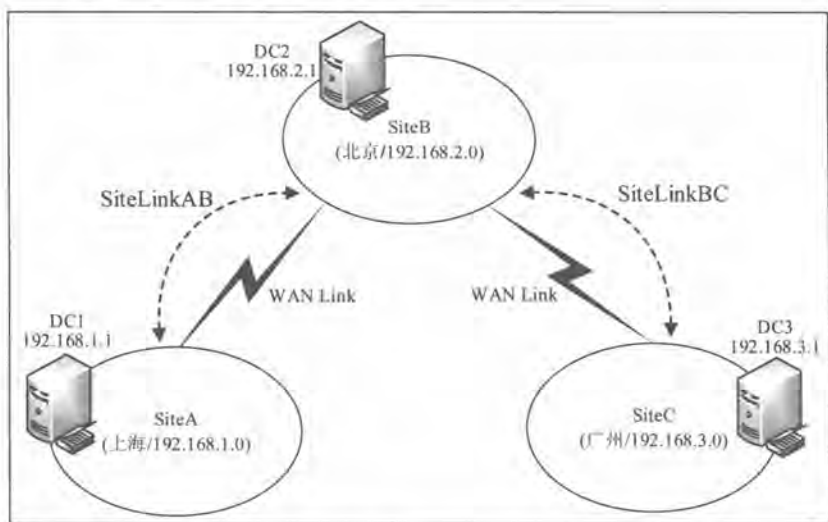


图 9-3-26

9.4 管理全局编录服务器

全局编录服务器（Global Catalog Server，GC）也是一台域控制器，其中的全局编录存储着林中所有AD DS对象，如图9-4-1所示。

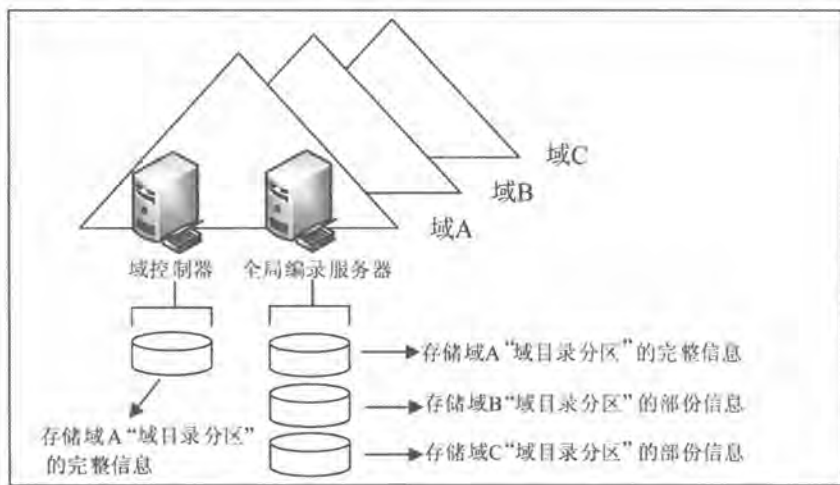


图 9-4-1

图中的一般域控制器内只会存储所属域内域目录分区的完整信息，但是全局编录服务器

还会存储林中所有其他域之域目录分区对象的部分属性，让用户可以通过全局编录内的这些属性，很快速找到位于其他域内的对象。系统默认会将用户常用来查找的属性加入到全局编录内，例如登录账户名称、UPN、电话号码等。

9.4.1 向全局编录内添加属性

也可以自行利用Active Directory架构控制台来将其他属性加入到全局编录内，不过可能需要在域控制器上先执行regsvr32schmmgmt.dll命令来登录schmmgmt.dll，然后再通过【按 $\text{Win}+\text{R}$ 键 \rightarrow 输入MMC后单击确定按钮 \rightarrow 单击文件菜单 \rightarrow 添加/删除管理单元 \rightarrow 选择Active Directory架构 \rightarrow 单击添加按钮】来建立此控制台。

如果要将其他属性加入到全局编录中的话：【如图9-4-2所示单击左侧的属性文件夹 \rightarrow 双击右侧要加入的属性 \rightarrow 如前景图所示勾选将此属性复制到全局编录】。



图 9-4-2

9.4.2 全局编录的功能

全局编录主要提供以下的功能：

- ✎ **快速查找对象：**由于全局编录内存储着林中所有域的域目录分区的对象的部分属性，因此让用户可以利用这些属性很快地找到位于其他域的对象。举例来说，系统管理员可以使用【单击左下角开始图标 \rightarrow Windows 管理工具 \rightarrow Active Directory管理中心 \rightarrow 如图9-4-3所示单击全局搜索 \rightarrow 将范围处改为全局编录搜索】的方法，通过全局编录快速地查找对象。



图 9-4.3

附注

全局编录的TCP端口号码为3268，因此如果用户与全局编录服务器之间被防火墙隔开的话，请在防火墙开放此端口。

- ✎ **提供UPN (user principal name) 的验证功能：**当用户利用UPN登录时，如果负责验证用户身份的域控制器无法从其AD DS数据库来得知该用户是隶属于哪一个域的话，它可以向全局编录服务器查询。例如用户到域sh.sayiis.local的成员计算机上利用其UPNgeorge@sayms.local账户登录时，由于域sh.sayiis.local的域控制器无法得知此george@sayms.local账户是位于哪一个域内（见Q&A），因此它会向全局编录查询，以便完成验证用户身份的工作。



如果用户的UPN为george@sayms.local，则该用户账户就一定是存储于域sayms.local的AD DS数据库吗？



不一定！虽然用户账户的UPN后缀默认就是账户所在域的域名，但是后缀可以更改，而且如果用户账户被移动到其他域时，其UPN并不会自动更改，也就是说UPN后缀不一定就是其域名。

- ✎ **提供通用组的成员信息：**我们在第8章讲过，当用户登录时，系统会为用户建立一个access token，其中包含着用户所隶属组的SID，也就是说用户登录时，系统必须得知该用户隶属于哪些组，不过因为通用组的成员信息只存储在全局编录，因此当用户登录时，负责验证用户身份的域控制器，需要向全局编录服务器查询该用户所隶属的通用组，以便建立access token，让用户完成登录的过程。

当用户登录时，如果找不到全局编录服务器的话（例如故障、脱机），则用户是否可以成功登录呢？

- 如果用户之前曾经在这台计算机成功登录过，则这台计算机仍然能够利用存储在其缓存区（cache）内的用户身份数据（credentials），来验证用户的身份，因此还是可以成功登录。
- 如果用户之前未曾在这台计算机登录过，则这台计算机的缓存区内就不会有该用户的身份信息，故无法验证用户身份，因此用户无法登录。

附注

如果用户是隶属于Domain Admins组的成员，则无论全局编录是否在线，他都可以登录。

如果要将某台域控制器设置为或取消为全局编录服务器的话：【如图9-4-4所示单击该域控制器☞单击NTDS Settings☞单击上方属性图标☞勾选或取消勾选前景图中的全局编录】。



图 9-4-4

9.4.3 通用组成员缓存

虽然应该在每一个站点内启用一台全局编录服务器，但是对一个小型站点来说，由于硬件配备有限、经费短缺、带宽不足等因素的影响，因此可能不想在此站点搭建一台全局编录服务器。此时可以通过通用组成员缓存来解决此问题。

例如图9-4-5中如果SiteB启用了通用组成员缓存，则当用户登录时，SiteB内的域控制器会向SiteA的全局编录服务器查询用户是隶属于哪些通用组，该域控制器得到这些数据后，便会将这些数据存储在缓存区内，以后当这个用户再登录时，这台域控制器就可以直接从缓存区内得知该用户是隶属于哪些通用组，不需要再向全局编录查询。此功能拥有以下的好处：

- 提高用户登录的速度，因为域控制器不需要再向位于远程另外一个站点的全局编录查询。



- ✎ 现有域控制器的硬件不需要升级。由于全局编录的负担比较重，因此需要比较好的硬设备，然而站点启用通用组成员缓存后，该站点内的域控制器就可以不需要对硬件升级。
- ✎ 减轻对网络带宽的负载，因为不需要与其他站点的全局编录来复制林中所有域内的所有对象。

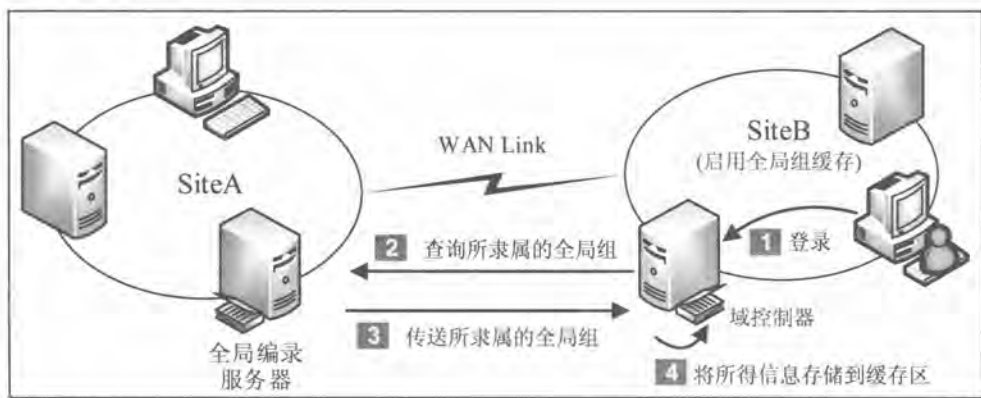


图 9-4-5

启用通用组成员缓存的方法为：【如图9-4-6所示选择站点（例如SiteB）选中右侧的NTDS Settings并右击属性选中启用通用组成员身份缓存】。



图 9-4-6

附注

域控制器默认会每隔8小时更新一次缓存区，也就是每隔8小时向全局编录服务器索取一次最新的信息，而它是从哪一个站点的全局编录服务器来更新缓存数据的呢？这可从图中最下方的启用通用组成员身份缓存（Refresh Cache from）来选择。



9.5 解决AD DS复制冲突的问题

AD DS数据库内的大部分数据是利用**多主复制模式**来复制的，因此可以直接更新任何一台域控制器内的AD DS对象，之后这个更新对象会被自动复制到其他域控制器。

但是如果两位系统管理员同时分别在两台域控制器建立相同的对象，或是修改相同对象的话，则之后双方开始相互复制这些对象时，就会发生冲突，此时系统应该如何来解决这个问题呢？

9.5.1 属性标记

AD DS使用**标记**（stamp）来作为解决冲突的依据。当修改了AD DS某个对象的属性数据后（例如修改用户的地址）后，这个属性的标记数据就会改变。这个标记是由三个数据所组成的：

版本号码	修改时间	域控制器的GUID
------	------	-----------

- ✎ **版本号码（version number）**：每一次修改对象的属性时，属性的版本号码都会增加。起始值是1。
- ✎ **修改时间（timestamp）**：对象属性被修改的原始时间。
- ✎ **域控制器的GUID**：发生对象修改行为的原始域控制器的GUID。

AD DS在解决冲突时，是以标记值最高的优先，换句话说版本号码较高的优先；如果版本号码相同，则以修改时间较后的优先；如果修改时间还是相同，再比较原始域控制器的GUID，GUID数值较高的优先。

9.5.2 冲突的种类

AD DS对象共有以下三种不同种类的冲突情况，而不同种类的冲突，其解决冲突的方法也不同：

- ✎ 属性值相冲突
- ✎ 在某容器内新建对象或将对象移动到此容器内，但是这个容器已经在另外一台域控制器内被删除了
- ✎ 名称相同

1. 属性冲突的解决方法

如果属性值发生冲突，则以标记值最高的优先。举例来说，假设用户**王乔治**的**显示名称**



属性的版本号码目前为1，而此时有两位系统管理员分别在两台域控制器上修改了王乔治的显示名称（如图9-5-1所示），则在这两台域控制器内，显示名称属性的版本号码都会变为2。因为版本号码相同，故此时需要以修改时间来决定以哪个系统管理员所修改的数据优先，也就是修改时间较晚的优先。



图 9-5-1

可以利用以下的repadmin程序来查看版本号码（参考图9-5-2）：

```
repadmin /showmeta CN=王乔治,OU=业务部,DC=sayms,DC=local
```

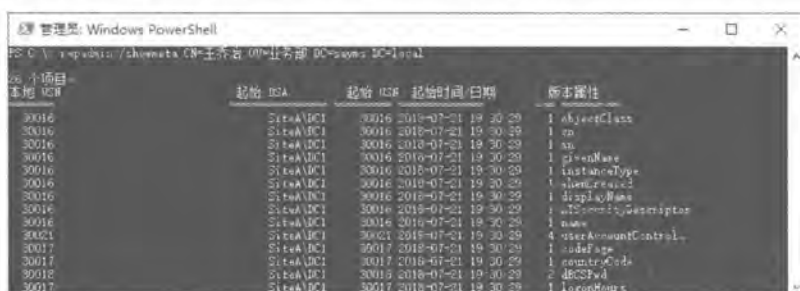


图 9-5-2

附注

Repadmin.exe还可以用来查看域控制器的复制拓扑、建立连接对象、手动执行复制、查看复制信息、查看域控制器的GUID等。

2. 对象存储容器被删除的解决方法

例如某位系统管理员在第1台域控制器上将图9-5-3中的组织单位会计部删除，但是同时第2台域控制器上却有另外一位系统管理员在组织单位会计部内新建一个用户账户高丽黛。请问两台域控制器之间开始复制AD DS数据库时，会发生什么情况呢？



图 9-5-3

此时所有域控制器内的组织单位**会计部**都会被删除，但是用户账户**高丽黛**会被放置到LostAndFound文件夹内，如图9-5-4所示。这种冲突现象并不会使用到标记来解决问题。



图 9-5-4

附注

若要练习验证上述理论的话，请先让两台域控制器之间网络无法通信，然后分别在两台域控制器上操作，再让两台域控制器能够通过网络正常通信、手动复制AD DS数据库。不过请先执行以下步骤，否则无法删除组织单位**会计部**：【打开**Active Directory管理中心**选中组织单位**会计部**并右击**属性**如图9-5-5所示单击组织单位节**取消勾选防止意外删除**】。



图 9-5-5



3. 名称相同

如果对象的名称相同，则两个对象都会被保留，此时标记值较高的对象名称会维持原来的名称，而标记值较低的对象名称会被改为：

物件的 RDNCNF：物件的 GUID

例如在两台域控制器上同时新建一个名称相同的用户赵日光，但是分别有不同的属性设置，则在两台域控制器之间进行AD DS数据库复制后，其结果为图9-5-6所示两个账户都被保留，但其中一个的全名会被改名。



图 9-5-6